Project No. 101083594
Call: DIGITAL-2021-SKILLS-01

Project start: 2022-12-01
Project duration: 39 months

CyberSecPro

D6.2
Report on Dissemination and Communication Activities

Document Identification	
Due date	2026-02-28
Submission date	2026-02-28
Version	1.0

Related WP	WP6	Dissemination Level	PU
Lead Participant	ACEEU	Lead Author	Thorsten Kliewe, Lina Landinez (ACEEU)
Contributing Participants	APRIO, ZELUS	Related Deliverables	D6.1, D6.3, D6.4, D6.5

Abstract: This deliverable reports on the implementation of dissemination and communication activities and thereby relates primarily to the Tasks 6.1 and Task 6.4 of the CyberSecPro project.

Co-funded by the
European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the European Health and Digital Executive Agency (HADEA) can be held responsible for them.

This document is issued within the CyberSecPro project. This project has received funding from the European Union's DIGITAL-2021-SKILLS-01 Programme under grant agreement no. 101083594.

Executive Summary

This deliverable (D6.2) reports on the dissemination and communication activities implemented within the CyberSecPro project up to Month 38 (M38). It presents the key communication assets (visual identity, templates and marketing materials, and the admin platform), the channels and formats used to reach target audiences, and performance against the Grant Agreement KPIs.

CyberSecPro established a coherent project presence through a partner-inclusive brand development process and a set of reusable dissemination templates, supported by an admin platform enabling structured reporting and real-time KPI monitoring. The project's digital dissemination generated particularly strong uptake of outputs: 9,076 total downloads were recorded, with deliverables accounting for 7,787 downloads (85.8%) and the project brochure for 507 — evidence of sustained demand for substantive technical materials and formal project documentation.

Social media matured into a high-performing dissemination channel, especially on LinkedIn (560 followers at M38, with strong impressions and engagement over the past year), complemented by a continued presence on X and a growing YouTube library supporting reusable outreach content. Event-based dissemination remained a core pillar, with 170 dissemination activities recorded across conferences, workshops, panels and other formats, and a strong scientific dissemination track with 56 publications documented by end of January 2026.

Stakeholder engagement was pursued as a strategic impact lever, not only to inform stakeholders, but to shape the wider cybersecurity skills ecosystem through standardisation, liaison and certification-oriented dialogue, contributing to the closing of the cybersecurity skills gap in Europe. The project engaged policy-making bodies and standardisation-relevant actors (including ENISA, ECCC, ESCO, ECSO, the European Commission and standards organisations), reaching more than 22 policy representatives, and collaborated with at least 45 EU-funded projects through clustering activities (e.g., joint workshops, conferences and co-authored outputs). This work strengthens the legitimacy, interoperability and potential long-term adoption of CyberSecPro results beyond the consortium.

Document information

Contributors

Name	Beneficiary
Thorsten Kliewe	ACEEU
Lina Landinez	ACEEU
Jeldo Meppen	ACEEU
Emmanouil Vergis	ZELUS
Elli Alimperti	ZELUS
Argyro Chatzopoulou	APIRO

Reviewers

Name	Beneficiary
Christos Douligeris	UPRC (Technical Lead)
Spiros Borotis	MAG (WP Lead)
Pinelopi Kyranoudi	TUC
Nuno Pedrosa	PDMFC

History

Version	Date	Contributor(s)	Comment(s)
0.1	2025-10-07	Thorsten Kliewe	First draft of ToC to plan data collection (internal)
0.2	2025-12-08	Lina Landinez	Second draft of ToC
0.21	2026-01-09	Lina Landinez	Introduction added
0.22	2026-01-15	Jeldo Meppen	Visual Identity added

0.23	2026-01-20	Lina Landinez	Templates, Admin Portal
0.24	2026-01-22	Lina Landinez	Website, Newsletter, Events, Dissemination Activities added
0.25	2026-01-31	Emmanouil Vergis	Social Media added
0.26	2026-02-02	Argyro Chatzopoulou	Stakeholder Engagement added
0.27	2026-02-05	Lina Landinez	KPI overview updated
0.3	2026-02-06	Lina Landinez, Thorsten Kliewe	Conclusion written
0.31	2026-02-11	Jeldo Meppen	Added acronyms, formatting changes, added Annex A and B
0.4	2026-02-25	Jeldo Meppen	Integrate feedback from the 1st review
0.5	2026-02-27	Jeldo Meppen	Update some numbers and feedback on the 2nd review
0.6	2026-02-28	Thorsten Kliewe	Finalisation and high-level review
0.7	2026-02-28	Spiros Borotis	Review and approval
1.0	2026-02-28	Atiyeh Sadeghi	Final check, preparation and submission process

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**AI**	Artificial Intelligence
C	**CDEB**	Communication, Dissemination, Exploitation & Business Growth
	CEN	European Committee for Standardization
	CENELEC	European Committee for Electrotechnical Standardization
	CSP	CyberSecPro
	CYS	Cyprus Organization for Standardization
D	**DCM**	Digital Curriculum Management
	DSA	Digital Security Authority (Cyprus)
E	**ECCC**	European Cybersecurity Competence Centre
	ECSF	European Cybersecurity Skills Framework
	ECSO	European Cyber Security Organisation
	ECTS	European Credit Transfer and Accumulation System
	ENISA	EU Agency for Cybersecurity
	ESCO	European Skills, Competences, Qualifications and Occupations
	ETSI	European Telecommunications Standards Institute
	EU	European Union
H	**HADEA**	European Health and Digital Executive Agency
	HEI	Higher Education Institution
	HRM	Human-Centric Risk Management
I	**ICT**	Information & Communications Technology
	IEC	International Electrotechnical Commission

	IPICS	Intensive Programme on Information and Communication Security
	ISO	International Organization for Standardization
K	**KPI**	Key Performance Indicator
N	**NCC**	National Coordination Centre
	NMIOTC	NATO Maritime Interdiction Operational Training Centre
S	**SME**	Small and Medium-sized Enterprise
	STEEP	Social-Technological-Economic-Environmental-Political
U	**UNITAR**	United Nations Institute for Training and Research
W	**WP**	Work Package

1 Introduction

1.1 Background

CyberSecPro is a 39-month initiative funded under the Digital Europe Programme, addressing the growing cybersecurity skills gap in Europe. Rapid digitalisation across critical sectors such as energy, health, maritime transport and public administration has significantly increased exposure to cyber threats, while the demand for qualified cybersecurity professionals continues to outpace supply.

Although European Higher Education Institutions (HEIs) offer a large number of cybersecurity degree programmes, these are often characterised by static curricula and limited hands-on training, making it difficult to respond to rapidly evolving market needs. CyberSecPro responds to this challenge by developing professional, practice-oriented cybersecurity training modules that complement existing academic offerings. The project strengthens collaboration between HEIs, industry, SMEs and public actors, enabling universities and training providers to play a more active role in upskilling the existing workforce and preparing new professionals for real-world cybersecurity challenges.

CyberSecPro brings together a large European consortium of universities, research organisations, SMEs and industry partners to design, deliver, evaluate and scale hands-on cybersecurity training modules. The project covers multiple industrial domains and emerging technologies and aims to establish CyberSecPro as a European reference model for professional cybersecurity education and training.

1.2 Purpose and Scope

This report documents and assesses the dissemination and communication activities implemented in the CyberSecPro project during the reporting period (up to M38). Its main purpose is to provide a structured overview of the actions carried out, the channels and tools used, the stakeholder groups reached, and the progress made against the project's communication and dissemination objectives.

In terms of scope, the report covers project-level dissemination and communication activities implemented by the consortium and reported under WP6, with references to related actions where relevant (e.g., activities supporting training uptake, stakeholder outreach, standardisation and liaison). It includes both quantitative and qualitative evidence, such as activity logs, communication outputs, stakeholder interactions, and KPI tracking.

The report is primarily descriptive and monitoring-oriented. It is intended to document implementation progress and provide transparency on communication and dissemination performance rather than to deliver an impact evaluation of the project. Likewise, while it may refer to exploitable results and sustainability-related actions where relevant for communication purposes, detailed exploitation planning and IPR-related matters are addressed in the corresponding WP6 deliverables.

1.3 Relation with other WPs and Deliverables

D6.2 consolidates and evidences the project's dissemination and communication work, reporting progress (iteratively, incl. M18 and M36) against the dissemination approach set in WP6.

- WP6 core linkage (planning → execution → reporting): D6.2 is the direct reporting output of Task 6.2 (Dissemination and Communication Activities) and is implemented in line with D6.1 (Dissemination, Communication Plan and Exploitation), which defines the channels, audiences and actions that D6.2 then reports against.
- WP2 & WP3 (what is being communicated): The "substance" disseminated via T6.2 and captured in D6.2 is grounded in the programme design and core technical assets (e.g. D2.1 - skills gaps, D2.2 - training technologies catalogue, D2.3 - programme specifications and D3.1 - programme main components, DCM and general-purpose curricula).
- WP4 & WP5 (evidence, uptake signals, and impact messaging): D6.2 is closely tied to the operational rollout and evaluation cycle, because dissemination increasingly relies on "what happened" and "what worked", drawing from WP4 training operations and reporting (e.g. D4.1

and the training-module reports linked to T4.3–T4.6) and from WP5 evaluation and best-practices consolidation (notably D5.2 based on T5.2–T5.3). These results enable credible communication of outcomes, participation, and lessons learned.

- The dissemination record in D6.2 also functions as a practical input to exploitation and sustainability work in WP6, supporting D6.3 (overall exploitation/sustainability/business plans) and, downstream, the grouped/individual exploitation outputs (D6.4 and D6.5) by documenting reach, stakeholder engagement, and market-facing visibility (incl. business events and policy-maker engagement described under T6.2).

1.4 Structure of the Report

This report is structured to provide a clear and evidence-based overview of the dissemination and communication work implemented in CyberSecPro up to Month 38 (M38). Following the introductory section, the document is organised into thematic sections that move from enabling resources, to implemented activities, to stakeholder-focused engagement, and finally to performance assessment and forward planning, in line with the deliverable's scope and table of contents.

Section 2 (Key Resources) presents the main communication assets and tools developed and used in CyberSecPro. It describes the project's visual identity, the templates and marketing materials created to ensure consistency across dissemination outputs, and the admin platform used to manage reporting and KPI monitoring.

Section 3 (Communication and Dissemination Activities) constitutes the core operational section of the report. It provides a detailed overview of the dissemination and communication actions implemented during the reporting period, organised by channel and activity type, including the website, newsletters, social media, CSP-hosted events, dissemination activities, and publications.

Section 4 (Stakeholder Engagements) focuses specifically on the activities implemented under Task 6.4 (Standardization, Liaison and Certification Activities). It outlines the methodological approach used, the identification of relevant stakeholder groups, and the implementation of engagement actions with policy makers, standardisation bodies, certification-related actors, and other European-funded projects.

Section 5 (Future Communication and Dissemination Activities) provides a forward-looking perspective by outlining communication and dissemination actions planned beyond M38, i.e. after the reporting period covered by this deliverable.

Section 6 (KPI Overview) summarises the key performance indicators used to monitor dissemination and communication effectiveness and provides a consolidated view of progress against the project's communication and dissemination targets.

Section 7 (Conclusion) concludes the report by reflecting on the overall dissemination and communication performance of the project, highlighting key achievements, lessons learned, and implications for the remaining project period and follow-up exploitation and sustainability efforts.

References and Annexes provide supporting information and supplementary material. In particular, the annexes contain the consolidated lists of dissemination activities and publications that underpin the analysis presented in the main body of the report.

2 Key Resources

2.1 Visual Identity

2.1.1 Brand Identity Development

Recognizing the critical importance of a cohesive brand identity for effective dissemination and communication, the CyberSecPro consortium invested significant effort in developing a distinctive visual identity through a collaborative, partner-inclusive process.

In early 2023, project partners participated in a workshop to articulate their vision and requirements for the brand. Based on this input, a designer created multiple logo concepts. The consortium selected the final logo through a two-stage voting process involving all team members. Following minor refinements and the creation of format-specific variants, core visual elements were established. These design standards formed the foundation for all subsequent marketing materials produced throughout the project lifecycle.

2.1.2 Visual Identity and Logo Design

The CyberSecPro logo combines symbolic elements that directly reflect the project's mission: developing cybersecurity professionals through education and upskilling. The design features an owl positioned within a shield, with an integrated open book element, set above the "CyberSecPro" wordmark (with "Pro" highlighted in gold).

The owl represents wisdom, vigilance, and analytical insight; qualities fundamental to effective cybersecurity professionals. In security contexts, owls symbolize the ability to detect threats others might miss, sharp analytical thinking, and persistent awareness. The shield reinforces themes of protection and security, while the book element emphasizes the educational foundation of professional development. The turquoise colour palette conveys trust and intellectual strength, while the gold accent on "Pro" highlights the project's focus on professional excellence.

This integrated symbolism effectively communicates CyberSecPro's core objective: cultivating knowledgeable, vigilant cybersecurity professionals who can protect organizations through expertise and continuous learning.

2.2 Templates & Marketing Materials

Based on the visual identity developed, various templates have been created:

Table 1: Templates

Format	File extension or Application
PowerPoint	.pptx
Report	.docx
Roll-up Banner	.ai

Format	File extension or Application
Poster	Canva
Flyer	Canva
Foldable Brochure	Canva
Wallpaper	.jpg
Newsletter	HubSpot

Based on these templates, various marketing and communication materials have been designed and used (see images below).

Figure 1: Foldable Brochure

Figure 2 Flyer

Figure 3 Poster

Figure 4 Rollup Banner

Figure 5 PowerPoint Template

Figure 6 Report Template

2.3 Admin Platform

To support the systematic management of dissemination and communication activities, the CyberSecPro consortium developed a dedicated admin platform, available at admin.cybersecpro-project.eu. The platform served as a central operational tool for collecting, managing and monitoring data related to communication, dissemination and training activities across the project.

In particular, the platform enabled structured management of website news, dissemination activities, publications, stakeholder engagements and implemented training modules, while providing real-time monitoring of key performance indicators (KPIs). This supported evidence-based decision-making, especially in relation to marketing and communication efforts, allowing the consortium to assess reach, engagement and effectiveness across different channels.

Overall, the admin platform played a key role in ensuring transparency, consistency and efficiency in tracking dissemination and communication performance, and acted as the main internal reference system for KPI monitoring throughout the project.

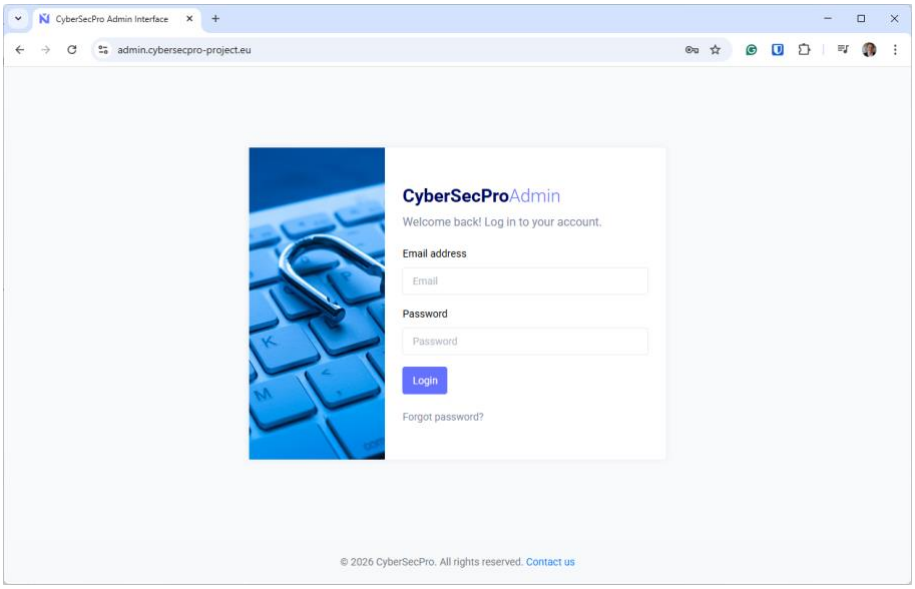


Figure 7: Admin Platform Login Page

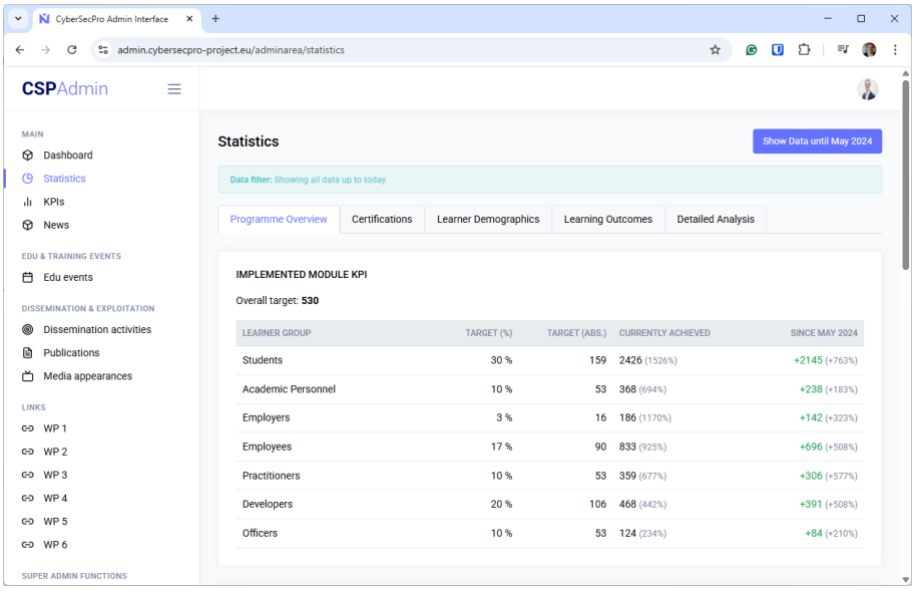


Figure 8: Admin Platform Statistics Page

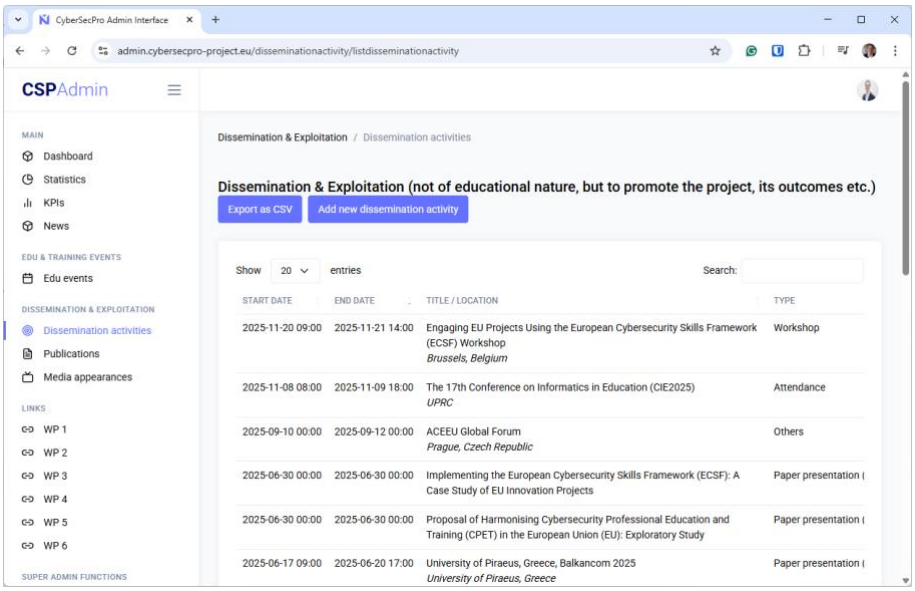


Figure 9: Admin Platform Dissemination Page

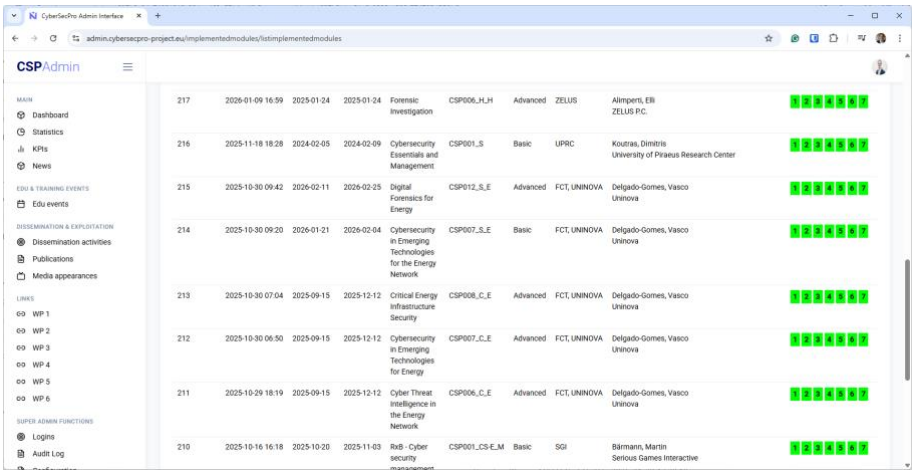


Figure 10: Admin Platform Implemented Modules Page

The CyberSecPro admin platform was actively used by 55 individual consortium members, recording a total of 2,412 logins over the project duration, demonstrating sustained engagement with the project's dissemination, communication and KPI monitoring processes.

3 Communication and Dissemination Activities

3.1 Website

The CyberSecPro website (www.cybersecpro-project.eu) served as the central digital hub for project information, resources, and stakeholder engagement throughout the project lifecycle. Designed to support educators, learners, and industry professionals, the website provided comprehensive access to project deliverables, training materials, news updates, and consortium activities. The platform effectively communicated the project's mission to advance EU cybersecurity competencies while maintaining consistent brand identity across all digital touchpoints.

Figure 11: CyberSecPro Website Screenshot

3.1.1 Website Structure

The CyberSecPro website featured a clear, user-focused navigation structure designed to facilitate access to project information and resources. The main navigation menu comprises five primary sections:

- **Home** – Landing page introducing the project's mission and key objectives
- **News** – Updates on project activities, events, and milestones
- **About** – Contextual information including:
  - About the project (objectives, scope, and approach)
  - Partners (consortium member profiles)
- **Activities & Outcomes** – Core project outputs organised by category:

- DCM (Digital Competence Matrix)
- Education & Training (course materials and programs)
- Publications (research outputs and articles)
- Deliverables (formal project reports)
- Dissemination (communication activities and outreach)

- **Contact** – Contact information and inquiry forms

The website header maintained consistent branding with the CyberSecPro logo and integrated social media links (LinkedIn, X/Twitter, YouTube) to facilitate cross-platform engagement. This structure provided intuitive access to different stakeholder groups; educators seeking training materials, learners looking for courses, and industry partners interested in project outcomes.

3.1.2 Website Statistics

Table 2: Website Statistics over project lifetime

Statistic	Total count
Unique visitors	2689
Page views	8180
Overall Downloads	9076
Brochure Downloads	507
Deliverable Downloads	7787

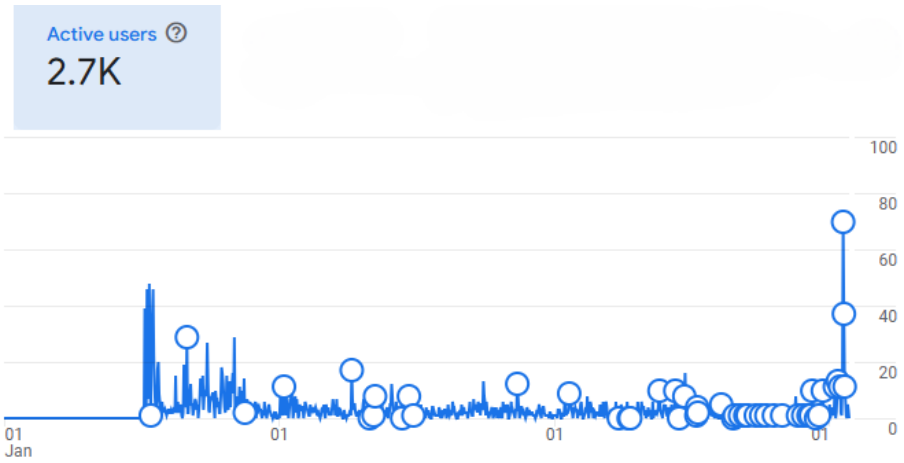


Figure 12: Active users from July 2023 (website launch) to Jan 2026

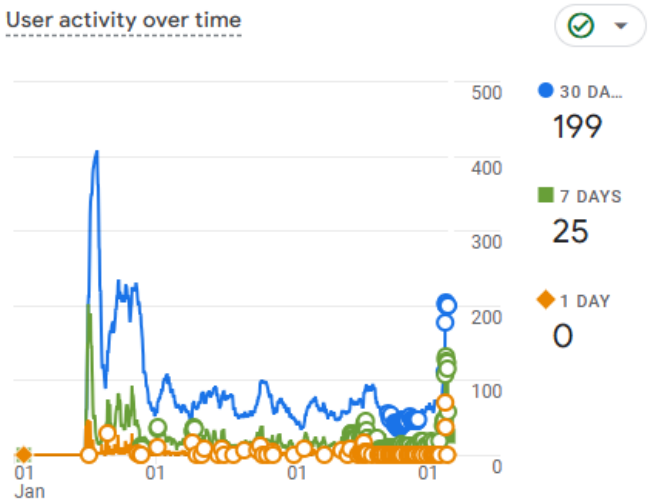


Figure 13: User activity over time

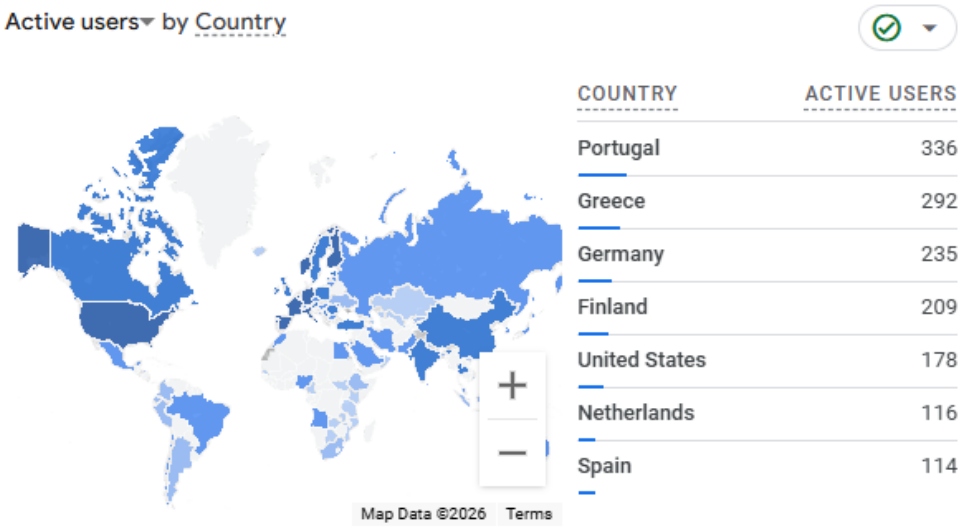


Figure 14: Active users by country

Views by Page title and screen class

PAGE TITLE AND SCREEN CLASS	VIEWS
CyberSecPro	3.9K
Education & Training – CyberSecPro	880
About – CyberSecPro	505
PartnersNew – CyberSecPro	498
News overview – CyberSecPro	431
Deliverables – CyberSecPro	404
News Detail – CyberSecPro	344

Figure 15: Views by Page

3.1.3 Website metrics evaluation

The website analytics demonstrate strong engagement and effective resource delivery throughout the project period. With 2,689 unique visitors generating 8,180 page views, the platform achieved an average of 3.04 pages per visitor. This indicates that users actively explored content rather than simply landing on the homepage. This engagement depth suggests the website successfully facilitated information discovery and navigation across project resources.

Download activity proved particularly robust, with 9,076 total downloads significantly exceeding unique visitor counts. This phenomenon reflects the project's multi-channel dissemination strategy: direct links to deliverables and resources were shared through consortium communications, partner networks, social media campaigns, and targeted email outreach. These direct-access URLs enabled users to download specific materials without necessarily navigating the main website, thereby generating downloads from users not captured in the unique visitor metrics. This approach proved highly effective for reaching specialized audiences who accessed resources through curated links rather than organic website discovery.

The distribution of downloads reveals clear user priorities: deliverables accounted for 85.8% of all downloads (7,787), while the project brochure generated 507 downloads. This pattern indicates strong interest in detailed technical outputs and formal project documentation, consistent with an audience of educators, researchers, and cybersecurity professionals seeking substantive materials.

The metrics validate both the website's functionality as a knowledge hub and the effectiveness of the project's broader dissemination strategy. The combination of direct-link sharing and website engagement ensured maximum reach across the European cybersecurity education community, successfully serving higher education institutions, training providers, and industry professionals invested in advancing EU cybersecurity competencies.

3.2 Newsletters

3.2.1 External newsletter

A project newsletter was initially developed as part of the CyberSecPro communication toolkit, fully aligned with the project's visual identity and implemented using the HubSpot platform. The first edition of the newsletter was released in summer 2023 and was disseminated to an initial group of stakeholders.

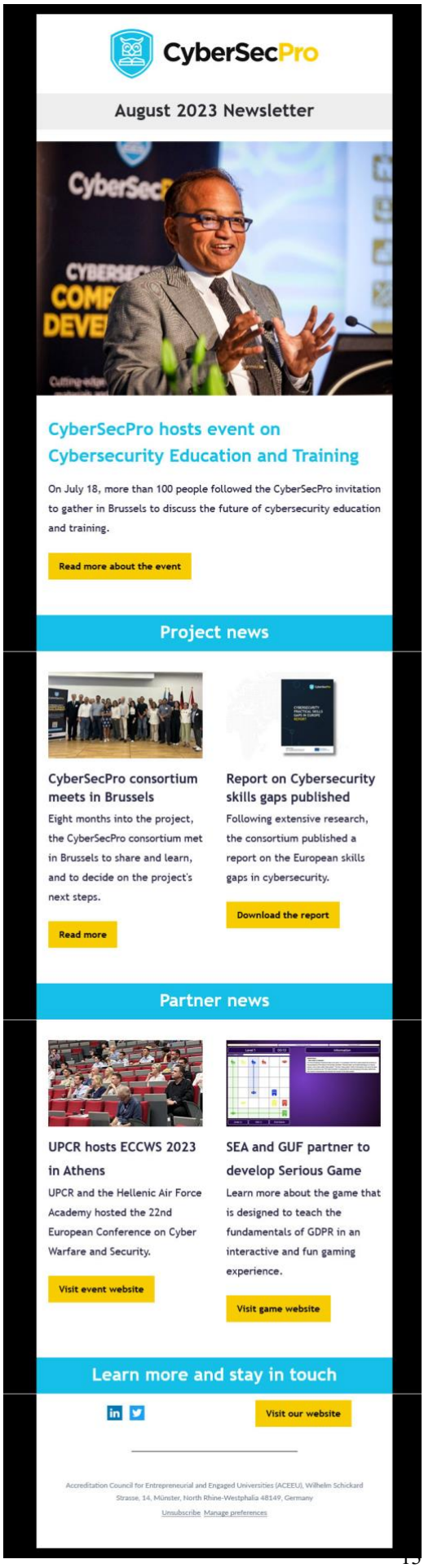
Subscriber acquisition was supported through multiple channels, including promotion at public events (using both paper-based subscription forms and online subscription forms made accessible through QR codes), as well as digital means such as direct invitations to professional contacts and project-related mailing lists. Despite these efforts, the growth in the number of subscribers remained limited. Subsequent dissemination activities and events did not lead to a significant increase in subscriptions, resulting in a low return on investment compared to the required time and coordination effort.

This issue was discussed during the project's mid-term review meeting with the Project Officer and the external reviewer. Their recommendations to discontinue the newsletter as a communication channel and to reallocate resources towards dissemination channels with broader reach and higher engagement potential, in particular social media and event-based communication, was followed.

This decision reflects the project's adaptive dissemination strategy and its commitment to focusing efforts on the most effective channels to maximise visibility and impact.

Table 3: Newsletter subscribers

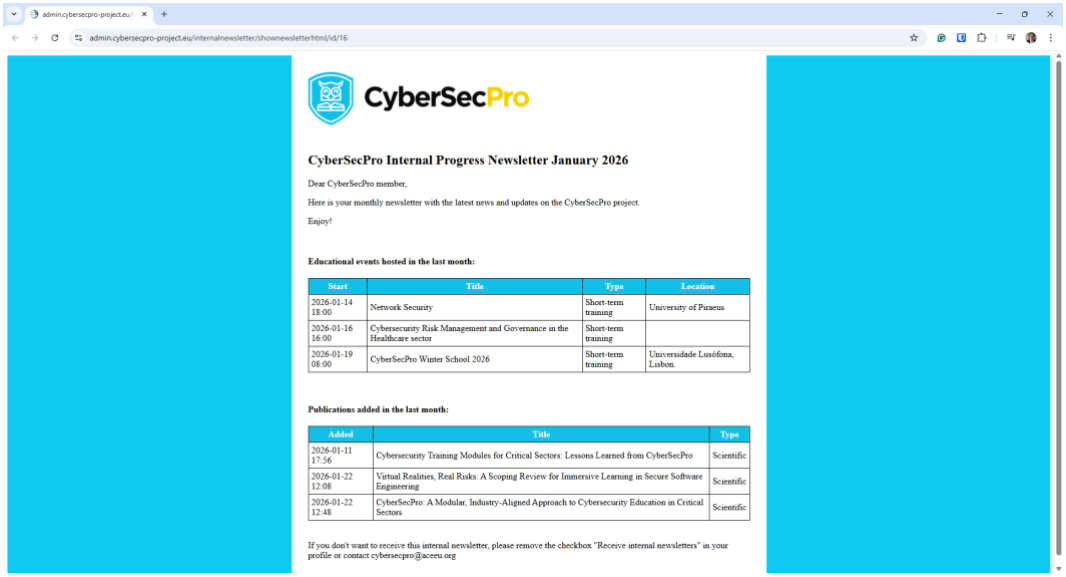
Target group	Subscribers
Educator	20
Employer	9
Learner	26
Policy / Government	10



3.2.2 Internal newsletter

In addition to the external newsletter, an internal monthly newsletter focused on project progress and achievements was introduced in November 2024 to support continuous internal communication within the CyberSecPro consortium. The newsletter highlights key activities, events and outputs from the preceding month and is automatically generated based on data entered into the CyberSecPro admin portal.

The internal newsletter is distributed to all registered CyberSecPro members via the admin platform and currently reaches 144 subscribers. By automating content generation and distribution, the newsletter ensured regular, low-effort internal communication and supported transparency, coordination and shared awareness of ongoing project activities across the consortium. This newsletter is directly addressing Measure 1.2 of the CDEB as stated in the Grant Agreement.



CyberSecPro

CyberSecPro Internal Progress Newsletter January 2026

Dear CyberSecPro member,

Here is your monthly newsletter with the latest news and updates on the CyberSecPro project.

Enjoy!

Educational events hosted in the last month:

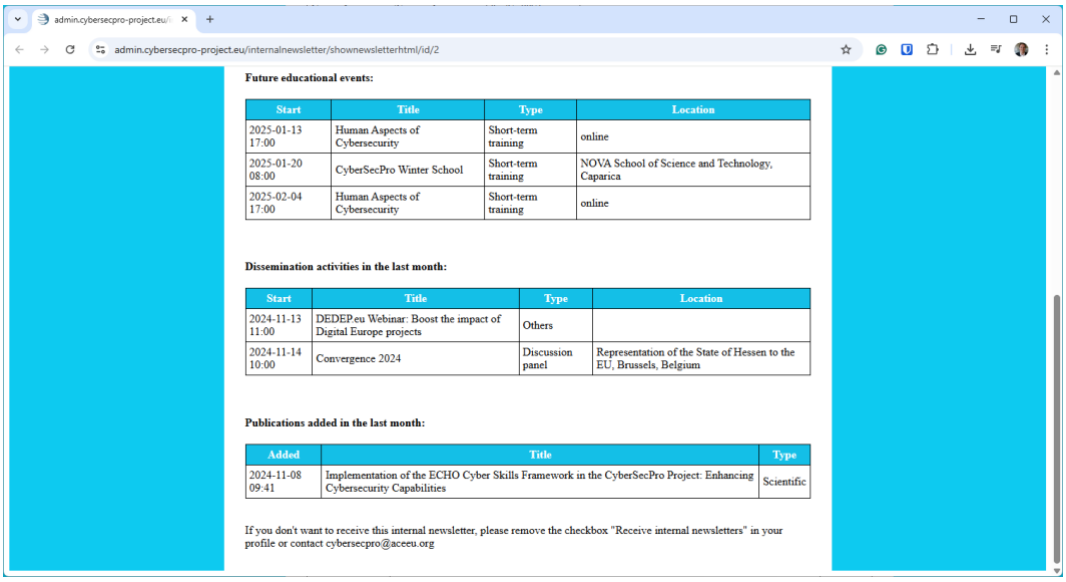
Start	Title	Type	Location
2026-01-14 18:00	Network Security	Short-term training	University of Piraeus
2026-01-16 16:00	Cybersecurity Risk Management and Governance in the Healthcare sector	Short-term training	
2026-01-19 08:00	CyberSecPro Winter School 2026	Short-term training	Universidade Lusófona, Lisbon.

Publications added in the last month:

Added	Title	Type
2026-01-11 17:56	Cybersecurity Training Modules for Critical Sectors: Lessons Learned from CyberSecPro	Scientific
2026-01-22 12:08	Virtual Realities, Real Risks: A Scoping Review for Immersive Learning in Secure Software Engineering	Scientific
2026-01-22 12:48	CyberSecPro: A Modular, Industry-Aligned Approach to Cybersecurity Education in Critical Sectors	Scientific

If you don't want to receive this internal newsletter, please remove the checkbox "Receive internal newsletters" in your profile or contact cybersecpro@aceeu.org

Table 4: Internal newsletter screenshot #1



Future educational events:

Start	Title	Type	Location
2025-01-13 17:00	Human Aspects of Cybersecurity	Short-term training	online
2025-01-20 08:00	CyberSecPro Winter School	Short-term training	NOVA School of Science and Technology, Caparica
2025-02-04 17:00	Human Aspects of Cybersecurity	Short-term training	online

Dissemination activities in the last month:

Start	Title	Type	Location
2024-11-13 11:00	DEDEP.eu Webinar: Boost the impact of Digital Europe projects	Others	
2024-11-14 10:00	Convergence 2024	Discussion panel	Representation of the State of Hessen to the EU, Brussels, Belgium

Publications added in the last month:

Added	Title	Type
2024-11-08 09:41	Implementation of the ECHO Cyber Skills Framework in the CyberSecPro Project: Enhancing Cybersecurity Capabilities	Scientific

If you don't want to receive this internal newsletter, please remove the checkbox "Receive internal newsletters" in your profile or contact cybersecpro@aceeu.org

Table 5: Internal newsletter screenshot #2

3.3 Social Media

Since the submission of the previous deliverable and up to the end of Month 38 (M38), the CyberSecPro project has significantly strengthened its social media presence, further consolidating its role as an effective dissemination and communication channel for project activities, results and events. Building on the foundations laid in the early stages of the project, social media channels have evolved into active platforms supporting outreach, engagement and visibility across the European cybersecurity ecosystem.

3.3.1 LinkedIn and X (formerly Twitter)

The CyberSecPro LinkedIn page has emerged as the primary and most impactful social media channel of the project. As of M38, the page has reached **557 followers**, representing an increase of +492 followers since the previous reporting period. Over the past year alone, LinkedIn activity has generated **13,561 impressions, 591 reactions**, alongside comments and reposts, indicating steady and meaningful engagement from a professional audience.

This strong performance reflects the platform's alignment with the project's target groups, including cybersecurity professionals, academics, students, policymakers and industry stakeholders. Numerous posts have been published to inform the community about key project developments, milestones, participation in conferences, organisation of workshops, winter and summer schools and other dissemination activities. Posting activity has been closely aligned with project evolution, ensuring that every significant update or event was communicated in a timely manner. LinkedIn has also been used consistently to promote and report on events organised by the project, thereby enhancing visibility and stakeholder participation.

In parallel, the CyberSecPro presence on X (formerly Twitter) has continued throughout the project, reaching **129 followers** (+115 since the early stages of the project). During the project's lifetime, the platform underwent a major transformation from Twitter to X, a change that has been accompanied by increased controversy and a noticeable decline in user engagement across the platform more broadly. This wider shift has affected interaction levels and overall dissemination performance, which is reflected in comparatively lower engagement metrics than those observed on LinkedIn. Nevertheless, the X account has remained active, supporting the dissemination of project updates, event announcements and retweets, contributing to a broader, even though limited, reach. The growth in followers and reposts demonstrates continued interest in CyberSecPro content despite the evolving landscape of the platform.

Across both platforms, a consistent visual identity and messaging strategy has been maintained, with systematic use of the project hashtag **#CyberSecPro**, reinforcing brand recognition and discoverability.

3.3.2 Dissemination of Events and Key Activities

Social media channels have played a central role in promoting and reporting on CyberSecPro's participation in and organisation of major events. Indicative examples include:

- Participation in the **CyberHOT Summer School** (Chania, September 2023), where social media posts highlighted the project's contribution to hands-on cybersecurity training and skills development at EU level.
- Organisation of the event **"Cybersecurity education and training – not why, but how?"** (Brussels, July 2023), focusing on practical approaches to cybersecurity education in the context of EU initiatives such as the EU Cyber Skills Academy and the ENISA ECSF framework. For further public CSP-hosted networking events, refer to section 3.4.1.
- **Focal Point Workshop for Universities: CyberSecurity Workshop** (online, December 2025), a two-day hands-on training targeting university student, covering red and blue team workflows and practical detection engineering using Microsoft Sentinel.

- **CyberSecPro Entrepreneurship Summit (final conference):** Innovation, Investment & Opportunities (Lisbon, January 2026), a highly successful event bringing together innovators, researchers, startups, SMEs, investors, and institutions to explore pathways from cybersecurity knowledge to market adoption.

For each of these activities, social media coverage included event promotion, dissemination of participation details, and post-event communication highlighting key outcomes, thus extending the impact beyond physical or virtual attendees.

3.3.3 Partner Engagement and Collaborative Dissemination

Partner engagement in CyberSecPro's social media activities has been encouraged throughout the project, supporting dissemination efforts in a complementary manner. Partners have contributed to dissemination primarily through resharing selected project-related content, tagging and the use of the common hashtag #CyberSecPro. This approach has supported consistency of messaging while allowing dissemination to extend beyond the project's core channels. Overall, this level of partner involvement reflects the collaborative nature of the project, while acknowledging that social media dissemination has been driven mainly through the project's official accounts.

3.3.4 YouTube Channel

Complementing the project's presence on LinkedIn and X, the CyberSecPro YouTube channel[1] has been actively populated and now hosts 45 videos, viewed aggregatedly around 500 times. The content includes interviews with academic staff and experts from partner organisations, as well as videos presenting and explaining the project's educational modules. This audiovisual material supports deeper engagement with project outputs, particularly in relation to training and educational content, and provides an accessible resource for students, educators, and professionals interested in cybersecurity skills development. The YouTube channel further strengthens the project's dissemination strategy by offering durable, reusable content aligned with CyberSecPro's objectives.

3.4 CSP-hosted Dissemination Events

3.4.1 Network events

A total of 7 self-hosted network events have been done.

Event 1: 19 January 2023, Brussels

A public launch event for the CSP project was hosted at the Hessen Representation to the EU in Brussel, attracting more than 100 participants. As part of the Launch event, a panel discussion on "Overcoming Cyberignorance: Capabilities, Skills, and Education in Cybersecurity" with a reception taking place to foster networking and knowledge exchange.

News link: https://www.cybersecpro-project.eu/index.php/news/?newsid=4

[1] https://www.youtube.com/@CyberSecProEU

Event 2: 18 July 2023, Brussels

More than 100 practitioners, government and association representatives, academics and citizens followed the invitation of the CyberSecPro consortium to join a discussion on the topic "Cybersecurity education and training – not why, but how?"

News link: https://www.cybersecpro-project.eu/index.php/news/?newsid=8


CyberSecPro

Event 3: CONVERGENCE 2023, 30 November–1 December 2023, Brussels

CONVERGENCE 2023 was a two-day single-track conference hosted at the Representation of the State of Hessen to the EU in Brussels, bringing together representatives from Trust in Digital Life (TDL), EU-CHECK, and CyberSecPro. The event focused on strengthening Europe's cybersecurity community by addressing capacity building, skills and education, research and innovation, and EU policy developments such as the AI Act, the Cybersecurity Resilience Act, and eIDAS 2.0. Sessions included expert panels, networking breaks, and an evening discussion on the challenges facing the European Cybersecurity Competence Centre (ECCC), fostering meaningful exchange among more than a hundred participants.

Link**:** https://trustindigitallife.eu/event/convergence-2023/

Event 4: 18 January 2024, Brussels

The CyberSecPro consortium hosted an evening event on the project, including a lively panel discussion focused on cybersecurity training and awareness ("Cybersecurity education and training – (how) can we help the European Cybersecurity Competence Centre?"). More than 80 people attended the evening at the Representation of the State of Hessen to the EU.

News link: https://www.cybersecpro-project.eu/index.php/news/?newsid=14



Event 5: CONVERGENCE 2024, 14–15 November 2024, Brussels

CONVERGENCE 2024 was a two-day gathering hosted at the Representation of the State of Hessen to the EU, uniting cybersecurity experts, researchers, and policymakers from across Europe. The programme included a pre-conference meeting with Armenian academic partners, followed by sessions on capacity building, digital identity, skills and education, and research and innovation. With contributions from ENISA, UNITAR, CNRS, universities, and industry experts, the event provided a platform for discussing governance, curricula, usability-by-design, business ROI, and Europe's evolving cybersecurity landscape, complemented by networking opportunities to support community building.

Link: https://trustindigitallife.eu/event/convergence-2024/

Event 6: 23 June 2025, Brussels

Hosted at the Representation of the State of Hessen to the EU, the event features a public panel discussion on "Which skills do we need for European digital sovereignty and its critical infrastructures?". The event brought together more than 85 cybersecurity professionals, policymakers, and academic experts.

Event 7: Convergence 2025

A one-day event held on 30 October in conjunction with project partners, EU-CHECK and CyberSecPro, hosted with the friendly support of the Representation of the State of Hessen to the EU at rue Montoyer 21 in Brussels. The event focused on the main drivers of digital transformation, from the impact of GenAI to the innovative initiatives that will determine our future.

The CSP participation among others included a session on "Skills for the Digital Economy: Aligning academic and industrial expectations and requirements". This panel looked at the challenges and opportunities in the cybersecurity industry, particularly in relation to talent and skills. While there is a growing pool of talent, the industry's fast pace and dynamic nature require innovative and agile responses to the workforce and skills gap. There is an important distinction to be made between the workforce and the skills gap, and the need for better mechanisms to ensure that the talent coming through the pipeline is equipped with the necessary skills and abilities.

Question discussed during the panel event included:

- Should companies be more open to hiring non-conventional talent and consider skills-based hiring?
- Is cybersecurity certification more important than developing a person's abilities or soft skills?

Speakers:

- Marc Vael, Chief Digital Trust Officer Esko Trust Center & President SAI.BE
- Spiros Borotis, Senior Product Manager/Analysts, Gruppo Maggioli
- Vanessa Lewis, Vice President of Recruitment, Nexova Group
- Wissam Mallouli, Chief Technology Officer, Montimage EURL

Moderator: Christos Douligeris, Professor, Department of Informatics, University of Piraeus Research Centre

Link: https://trustindigitallife.eu/event/convergence-2025

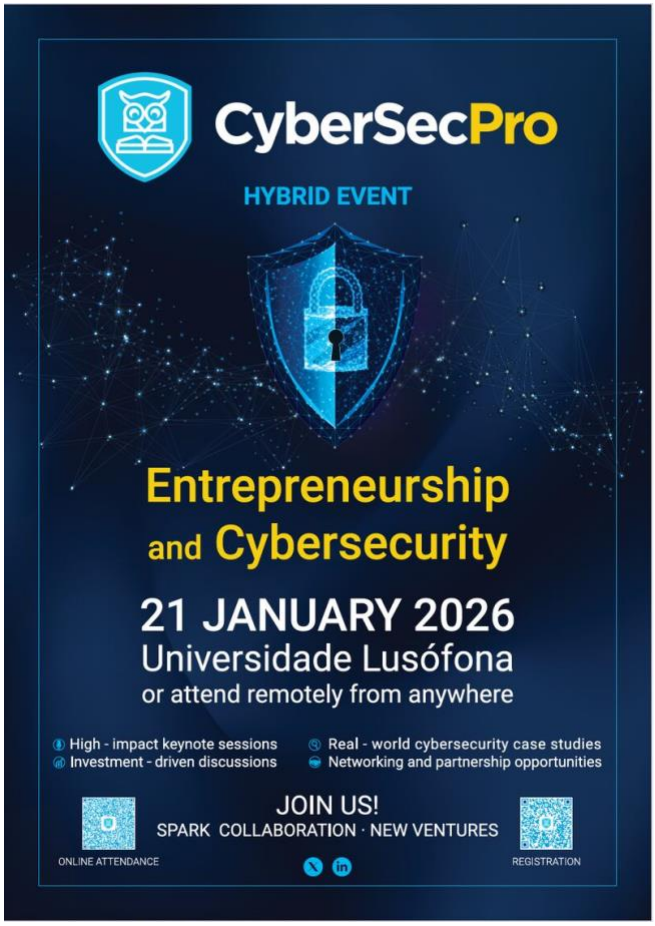
3.4.2 Final Conference

A one-day final conference was hosted in a hybrid format on January 21st in Lisbon, Portugal, hosted by Lusofona University. A total of 91 attended in person, with an additional 99 participants joining online.

The event featured a rich agenda, connecting CyberSecurity with Entrepreneurship. The opening of the conference was done by the coordinator of the CSA project LEADSx2030, supporting all projects of the call for proposals through which CyberSecPro was funded.

Wednesday, 21.01.2026

09:30-10:00	Registration and Welcome	
10:00-10:30	Advanced Digital Skills - current state of play the key role of cyber skills	**Brendan Rowan,** Managing Consultant at BluSpecs
10:30-11:00	CyberSecPro – Advancing cybersecurity skills in critical application domains. Q&A Session	**Kai Rannenberg** (Prof. Goethe University Frankfurt - GUF)
11:00-11:15	Networking Coffee Break	
11:15-12:15	Panel discussion: One European Cyber Talent Space on Standards, Skills and Education. Q&A Session	**Rodica Tirtea** (Senior Policy Officer, ECCC) **Cyber Security Centre in Portugal** **Evangelos Ouzounis** (ENISA) Moderator: Prof. Kai Rannenberg
12:15-12:45	Keynote on Venture Capital and Cybersecurity Startups. Exploring how investors identify and nurture breakthrough innovations in cybersecurity. Q&A Session	**Pedro Silva** (Founder and CEO of **ActiveCap)**
13:00-14:15	Networking Lunch Break	
14:30-15:30	Panel discussion: Emerging Technologies and Cybersecurity (AI, Quantum technologies and 6G) How cutting-edge technologies are reshaping the security landscape and business models. Q&A Session	**Luis Ribeiro** (CTO and Founder PDM) **Sokratis Katsikas** (Prof. NTNU) **Catarina Cabral Bastos** (Head of Indra Space) **José Neves** (AED cluster) Moderator: Dr. Luis Campos
15:30-16:00	Entrepreneurship Storytelling: Lessons from Building a Tech Business. A personal journey through innovation, resilience, and growth. Q&A Session	**Karolina Attspodina** (CEO of WeDoSolar)
16:00-17:00	Startup Launchpad for Cybersecurity Skills, Regulation and Go-to-Market Readiness Q&A Session	**Pedro Silva** (Founder and CEO of **ActiveCap)** **Domingos Cruz** (Managing Partner of CCA) **Herman Ruiz Ocampo** (Ecole Des Ponts Business School) Moderator: Dr. Emmanouil Vergis


CyberSecPro
HYBRID EVENT
Entrepreneurship
and Cybersecurity
21 JANUARY 2026
Universidade Lusófona
or attend remotely from anywhere
High - impact keynote sessions
Investment - driven discussions
Real - world cybersecurity case studies
Networking and partnership opportunities
JOIN US!
SPARK COLLABORATION · NEW VENTURES
ONLINE ATTENDANCE
REGISTRATION


7 EDUCATIONAL OFFERINGS


Cybersecurity Funding


ECCC
ECCC & Cybersecurity
Investments

3.5 Dissemination activities

By the end of January 2026, a total of **170 dissemination activities** had been recorded in the CyberSecPro admin portal. These activities comprise **55 attendance events, 50 paper presentations** (47 on-site and 3 online), **18 workshops, 17 discussion panels,** and **30 other activities**, reflecting sustained engagement across diverse professional and academic channels.

In terms of accessibility, **137 activities** were limited-access events targeting specific stakeholder groups, while 33 were open to the public free of charge. This distribution indicates a strong focus on targeted dissemination within professional and expert communities, complemented by broader public outreach efforts to extend the visibility and impact of CyberSecPro results.

The full list of dissemination activities can be found in Annex A.

3.6 Publications

By the end of January 2026, a total of **56 publications** had been produced within the CyberSecPro project and recorded in the admin portal. These outputs include 10 journal articles**,** 44 conference papers, 1 report, and 1 other publication (short paper), reflecting active dissemination of project results through established academic and professional channels.

In terms of target audience, 49 publications are scientific, addressing the research community, while 2 publications are practitioner-focused and 5 publications are classified as other outputs, supporting broader knowledge transfer. This publication portfolio demonstrates a strong emphasis on scientific dissemination, complemented by additional formats to extend the reach and applicability of CyberSecPro results.

The full list of publications can be found in Annex B.

4 Stakeholder Engagements

4.1.1 Introduction to Task 6.4.

This section presents the activities implemented as part of Task 6.4. Standardization, Liaison and Certification Activities. This task brings together 9 of the partners of the project to interact with stakeholders in a regular fashion and pave the way for certified professional practical training programs that serve the market needs.

In Deliverable 6.1. Dissemination, Communication Plan and Exploitation, (Section 1.2) the project has identified several key stakeholders to address. Specifically, within the relevant section, the following target audiences are identified:

1. Security services and/or training providers: These organizations can benefit from using or licensing CyberSecPro solutions to enhance the security or privacy-preserving capabilities of their products and services;
2. Enterprises and Small and Medium-sized Enterprises (SMEs): CyberSecPro solutions offer significant value to enterprises and SMEs, enabling them to increase their workforce competence that is critical to develop secure products, and services;
3. Academia: contribute to their training and education activities in the area of cybersecurity and increase the capability to build a new generation of skilled researchers and practitioners;
4. Policy-making bodies (certification stakeholders, ministries of education, National Cybersecurity Competence Centres, ENISA, ECCC): impact standardisation and policy-making activities around cybersecurity training and education capabilities;
5. Individual trainees and practitioners: Individuals will benefit the CyberSecPro solutions to increase their skills and competences;
6. General public: The general public is also a target audience for CyberSecPro. The objective here is to raise awareness about the importance of security in their daily activities and encourage them to adopt CyberSecPro techniques and tools. This engagement helps in delivering a secure, resilient, and digital Europe.

Task 6.4 focuses on the activities performed to disseminate, communicate and engage Policy-making bodies (as described above) in relation to the activities and outcomes of the project. Additionally, as prescribed in the Grant Agreement, the task also focuses on activities that could be implemented in collaboration with other European-funded projects, to increase awareness of the results of the project and strengthen the impact and message of the CyberSecPro project.

4.1.2 Connection to the CDEB objectives and KPIs

As already discussed in Deliverable 6.1, the project's Communication, Dissemination, Exploitation and Business growth (CDEB) plan has four objectives, each of which requires accompanying communication measures and KPIs to monitor success. This task is connected directly with the following CDEB objectives and specific measures:

CDEB Objective 1 | Raise national and international awareness of the project and its objectives and the ways in which to participate in CyberSecPro hands-on training activities. Drive demand among individual trainees and world class trainers, European High Education Institutions, cybersecurity companies and industries, researchers and innovators

> Measure 1.5: Early contact with key work groups (e.g. consortia from similarly themed projects, digital skills initiatives, EC institutions) will be incrementally made to discuss collaboration opportunities through scoping ways to foster the project impacts.
>
> Target group: Participants, project partners and relevant stakeholders active in Horizon EU/ CEF/ENISA, Erasmus+, COSME, DG EMPL, DGCNECT projects and initiatives related to cybersecurity digital skills to initiate synergies and collaborations for results promotion, co-organise events and formulate an enhanced educational agenda that can link to external agendas (e.g. the EU agenda);

KPIs: >10 similarly themed projects and initiatives identified; >5 jointly organized workshop.

CDEB Objective 2 | Establish mechanisms to not only transfer knowledge among the consortium partners and those external to the project, but also to exchange crucial knowledge as part of a two-way process.

Measure 2.4: Public consultation and policy events involving policy makers and relevant working groups (identified through e.g. policy fellowship schemes) will be closely monitored and results will be presented in open national and international networking events in order to boost reciprocal relationships between students, academics, sectoral specialists, researchers, industry and policy makers (e.g. Ministries of Education) focusing on crucial advance trainings of digital skills. The aim is to let them know the progress accomplished in CyberSecPro and influence them to capitalise on the project results and on the demonstrator outcomes and best practices identified.

Target group: Policy makers (national ministries, governmental officers, councils, EU, National, Regional and Local Authorities (NRLA), Regulatory Agencies, Standardisation Organisations e.g., ETSI, CEN, ISO), EU Institutions and agencies (e.g. DG CNECT, DG EMPL, ENISA, JRC, ECSO) to evaluate the project's Social Technological, Economic-Environmental-Political (STEEP) aspects, define future training, education, research and innovation directions and provide input for standardization activities.

KPIs: >50 hard copies distributed in >5 events; engagement of >7 policy making bodies;

4.1.3 Task methodology

Task 6.4 covers three topics: Standardization, Liaison and Certification. During the first stages of the project, a methodology was developed to support the effective implementation of all the activities and objectives of the task. This methodology consisted of five distinct steps, as depicted in Figure 16.

- Step 1 – Analysis: During this step, the scope, purpose, objectives, KPIs and rationale of the task were analysed.
- Step 2 – Identification of target audience: For each one of the topics and objectives of the task, the target audience was identified.
- Step 3 – Identification of opportunities: The project partners, continuously search for or create opportunities to communicate and engage the target audience for the topics of the task with the aim to support and effectively achieve the objectives of the task.
- Step 4 – Implementation of actions: Suitable activities are implemented, taking advantage of the opportunities identified or created.
- Step 5 – Lessons learned & Improvement: Each activity performed is analysed after its completion and any feedback relevant and useful for the project is identified and provided back to the project.

Figure 16: Task 6.4 methodology

4.1.4 Implementation of the task methodology

ANALYSIS

The task focuses on activities related to Standardization, Liaison with policy makers involved in cybersecurity skills and Certification. This section provides the analysis of scope and purpose for each one of these three components.

STANDARDIZATION:

ISO/IEC Guide 2:2004 describes standardization as the:

> activity of establishing, with regard to actual or potential problems, provisions for common and repeated use, aimed at the achievement of the optimum degree of order in a given context.

Note 1 to entry: In particular, the activity consists of the processes of formulating, issuing and implementing standards.

Note 2 to entry: Important benefits of standardisation are improvement of the suitability of products, processes and services for their intended purposes, prevention of barriers to trade and facilitation of technological cooperation.

Within this context, standardisation in the area of cybersecurity skills relates to efforts focused on providing a common and recognized framework for reference, communication and interoperability. In this area, the CyberSecPro project has identified a number of documents from national, European and international actors and has documented them as part of Deliverable 2.1. There are other documents and standards that relate to education and training, such as ISO 21001:2025, ISO 29995:2021 and others but they are more generic and extend outside the scope of the activities and purpose of the project.

LIAISON WITH POLICY MAKERS:

Based on the Cambridge dictionary, Liaison means:

> communication between people or groups who work with each other.

Within the scope of Task 6.4, the term liaison shall mean the activities where a message regarding the CyberSecPro project, is directly communicated to the selected interested parties. For example, a meeting or an event, where the outcomes and messages of the CyberSecPro project are presented with the attendance or the interaction with or the co-organization of a specific person from an interested party, shall be considered liaison.

CERTIFICATION:

ISO/IEC 17024:2012 defines the certification process as:

> activities by which a certification body determines that a person fulfils certification requirements, including application, assessment, decision on certification, recertification and use of certificates and logos/marks.

The CyberSecPro project, does not undertake formal certification as defined by ISO/IEC 17024:2012 (acting as a third-party certification body), but has produced two deliverables in the area of Certification. Specifically, as part of the design activities of WP3, the project has proposed Deliverable 3.2 - CyberSecPro Cybersecurity Certification Schema Proposal and as part of the multifaceted evaluation, best practices and benchmarking activities of WP5, deliverable D5.3 – CyberSecPro certification schema. In Deliverable 3.2., three schemes are proposed which namely are: Scheme A: Sector-agnostic scheme for a professional cybersecurity programme, Scheme B: Descriptions of the 12 training modules, and Scheme C: Syllabi of the 12 training modules. Whereas Deliverable 5.3, is the mature version of D3.2, after the various implementation activities, meaning that this deliverable contains the final proposed Cybersecurity certification scheme for practical cybersecurity programs accompanied with ECTS proposed scales and a possible interoperability framework.

Task 6.4 complements the relevant WP3 and WP5 tasks and deliverables, by communicating and engaging stakeholders in the subject of Cybersecurity Skills Certification.

4.1.5 Identification of target audience

STANDARDIZATION:

After the analysis of the scope of standardization as part of the CyberSecPro project, the key audience were identified. In this case they include:

ENISA

Capacity building Unit

The Capacity Building Unit, is related to the following ENISA activities:

ENISA addresses capacity building across the spectrum. It starts by investing in youth through competence building and training, whilst providing continuous upskilling and reskilling opportunities to professionals, to keep up with the fast-changing nature of cybersecurity. The focus is not only on increasing cybersecurity skill sets in Member States and contributing to the objectives of the Cybersecurity Skills Academy, but also on making sure that the various operational communities always possess the appropriate capacity to deal with the cyber threat landscape. Engaging closely with key players and multipliers in the EU is crucial to ensuring adequate preparedness across sectors and borders, effectively using the lessons learned from well-planned exercises.

Ad-Hoc Working Group on the European Cybersecurity Skills Framework (2023-2025)

The scope of this ad hoc working group is to assist ENISA in the governance, implementation and future evolution of the European Cybersecurity Skills Framework (ECSF).

Key tasks of this ad hoc working group include:

- act as an ambassador to facilitate the implementation of the ECSF in their own organization and/or partner organisations;
- support the governance of the ECSF (monitor endorsement, implementation, and support maintaining the ECSF registry);
- support in the promotion of the ECSF (participation in webinars, conference, etc.);
- assist in the implementation of the ECSF, propose and evaluate changes to the ECSF or other corrective actions;
- review related ENISA documents supporting the ECSF.

ISO

ISO/IEC JTC 1/SC 27

The scope of this committee covers the development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management systems, security processes, and security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;
- Conformance assessment, accreditation and auditing requirements in the area of information security management systems;
- Security evaluation criteria and methodology.

SC 27 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas

CEN/CENELEC

CEN/CLC/JTC 13

CEN-CLC/JTC 13 'Cybersecurity and data protection' is the CEN and CENELEC horizontal technical committee that addresses these needs. Its primary objective is to transport relevant international standards (especially from ISO/IEC JTC 1 SC 27) as European Standards (ENs) in the Information Technology (IT) domain. It also develops 'homegrown' ENs, where gaps exist, in support to EU regulations (RED, eIDAS, GDPR, NIS, etc.). These two streams of activities aim at creating a strategic portfolio of standards in Europe, which fits the European needs. CEN-CLC/JTC 13 works closely with ENISA (The European Union Agency for Cybersecurity) in the context of the European certification schemes, and with the European Commission, in the frame of the cybersecurity-related standardization request under the Radio Equipment Directive (RED).

CEN/CLC/JTC 21

CEN-CENELEC Joint Technical Committee 21 (JTC 21) is a dedicated body focused on standardization in the field of Artificial Intelligence (AI). This committee plays a crucial role in developing European Standards for AI technologies, addressing the unique needs and requirements of the European market and societal context.

The committee's work is particularly important as AI technologies continue to evolve and impact various sectors across Europe. By developing harmonized standards, JTC 21 aims to support the implementation of AI systems that are not only technologically advanced but also align with European values and regulatory frameworks like the AI Act.

ETSI

TC CYBER is recognized as a major trusted centre of expertise offering market-driven cyber security standardization solutions, advice and guidance to users, manufacturers, network, infrastructure and service operators and regulators. ETSI TC CYBER works closely with stakeholders to develop standards that increase privacy and security for organizations and citizens across Europe and worldwide. We provide standards that are applicable across different domains, for the security of infrastructures, devices, services, protocols, and to create security tools and techniques.

DIN

DIN Standards Committee Information Technology and Applications (NIA)

The Information Technology and Applications Standards Committee (NIA) is part of the DIN German Institute for Standardization and is the official national body for standardization in information technology and in selected application areas of information technology.

The NIA develops standards in the field of information technology and selected areas of application of information technology. The standards of information technology aim to:

- Improve the performance and quality of IT systems,
- To increase the security of IT systems and data,
- support the portability of application programs,
- ensure the interoperability of IT products and systems,
- Unify development environments
- and to design the user interfaces ergonomically.

The areas of application that are dealt with in the DIN Standards Committee for Information Technology and Applications include:

- Office organization and office technology,
- postal services,
- Banking,
- Electronic business

- as well as the exchange of data and information in the administrative and logistical chain of the movement of goods in the consumer goods industry.

CYS

The Cyprus Organization for Standardization (CYS) is the National Standardization Body of Cyprus, since January 1, 2005, and is responsible for all Standardization activities based on Law 156 (I)/2002. CYS operates as a limited liability (Ltd) organization, with the Republic of Cyprus being the sole shareholder. It is governed by a Board of Directors appointed by the Council of Ministers and consists of high-calibre personalities of the Cypriot society.

CYS actively participates in International and European Standardization as a full member of the International Standardization Organizations ISO and ITU, as well as the European Standardization Organizations CEN, CENELEC and ETSI. CYS represents Cyprus in European and International Technical Standardization Committees as an equal member, always aiming to safeguard the national interests.

LIAISON WITH POLICY MAKERS:

As defined in Deliverable 6.1, under the term policy makers, a variety of stakeholders is represented. Such stakeholders are for example: certification stakeholders, ministries of education, National Cybersecurity Competence Centres, ENISA, ECCC and also European funded projects in the field of cybersecurity education, training or certification.

The project undertook a structured approach to the identification and extracted a list of interested parties. This list contains different types of stakeholders (including projects), consists of 171 entries and will not be depicted here in detail. Instead, depicts the main categories of the identified stakeholders, the number of stakeholders identified within each category and indicative examples of members identified.

Table 6: Classification of identified policy makers

Category of interested party	Number identified	Indicative examples
Professional Certification Bodies	6	ISACA, SANS, ISC2, CompTIA, EC-Council, CREST
European Policy Makers	17	Europol, CEPOL, ECTEG, ENISA, ESDC, ECSO, ESCO, EEAS, DG EMPL/CNECT, DIGIT, CERT-EU, HADEA, ECCC
International Policy Makers	2	United Nations Institute for Training and Research (UNITAR), IEEE
National Policy Makers	17	Centre for Cybersecurity Belgium (CCB), Digital Security Authority (DSA) of Cyprus, National Cyber and Information Security Agency (Czech Republic), National Coordination Centre for Cybersecurity - Federal Office for Information Security (BSI)
European-funded projects in the area of education and training	129	CADMUS, AKADIMOS, CyberPro Train, CyberSec4OT, CYCERONE, NERO, SMARCO, CyberFort, CURIUM, CyberHubs, CyberFort, CyberAgent, CyberMACS

As seen from the table above, 129 European-funded projects have been identified. These projects have received funding from different European programmes, mainly ERASMUS+ and DIGITAL and all are related to education and training connected to cybersecurity skills. By identifying 129 projects, the project has surpassed the KPI of Measure 1.5, i.e., >10 similarly themed projects and initiatives identified.

CERTIFICATION:

The audience related to certification, as it concerns the CyberSecPro project, is a varied one. It consists of Professional Certification Bodies, European Policy Makers and European funded projects in the area of education and training as identified in Table 7.

4.1.6 Identification of opportunities and implementation of actions

ENISA

In December 2022, ENISA launched a call for an Ad Hoc Working Group on Cybersecurity Skills Framework with the aim to assist ENISA in the governance, implementation and future evolution of the European Cybersecurity Skills Framework (ECSF). The CyberSecPro members identified this opportunity early on, submitted an application and have been a permanent observer of this group since early 2023. The ED DECISION No 10/2023 has established the ad-hoc group and ED DECISION No. 48/2025 lists of updated candidates for membership.

By joining the ad-hoc working group, the project teams had the ability to be informed, involved in the group's activities in relation to the ECSF and to provide direct feedback from the project.

The activities included:

- The project participated in the provision of feedback on the ECSF (07/06/2024 – Contribution ID: 84d70c21-1b06-4d95-a057-55d8ca2b8681). The feedback included information on how the CyberSecPro project has utilized the ECSF, communicates the CyberSecPro approach for building related curricula and training courses, describes the proposal for three certification schemas and provides recommendations on the improvement of the ECSF. This last part is included as reference also in Error: Reference source not found of this document.
- The project participated in all ad-hoc working group meetings, both virtual and online.
- The project attended the European Cybersecurity Skills Conference 2023 and the European Cybersecurity Skills Conference 2024.
- The project co-organized the European Cybersecurity Skills Workshop. As highlighted in the Communication on the Cybersecurity Skills Academy, the ECSF is the EU reference framework for cybersecurity skills. Alignment of education, training, and workforce development with the ECSF strengthens comparability, improves skills' gap tracking, and contributes to a more cohesive skills ecosystem. The purpose of the workshop aimed to address the following:
    - Align stakeholders around ECSF implementation strategies
    - Encourage peer exchange and mutual learning
    - Showcase ECSF practical use cases and project results
    - Identify challenges, gaps, and future priorities
    - Strengthen collaboration across the EU cybersecurity skills landscape

The workshop participants were determined following a suitable call for speakers. The workshop includes the following two types of activities: 1) presentations of projects and discussions on projects developments and 2) an interactive exercise between the participants on the following four thematic areas: Designing and Delivering Training Activities for Specific Workforce Sectors, Designing and Delivering Horizontal Training and Education Initiatives, Analysis of Cyber Skills Gaps in the Workforce and Types of Cyber Skills Certificates.

Within the European Cybersecurity Skills Workshop, the CyberSecPro project participated and engaged stakeholders in the following ways:

1. Ms. Chatzopoulou from APIRO, provided a presentation entitled « CyberSecPro: training courses aligned to ECSF». The presentation described how the design of the CyberSecPro training programme was connected to the ECSF, the details on the methodology employed by the project to produce the key knowledge areas and the structure of the sector specific training programmes and the proposals for the certifications schemas for sector specific trainings.

Figure 17: Photograph from the beginning of the presentation of CyberSecPro in the European Cybersecurity Skills Workshop

2. Ms. Chatzopoulou from APIRO coordinated (along with the representative from the Agenzia per la Cybersicurezza Nazionale, Italy) discussions on the Types of Cyber Skills Certificates within the interactive exercise and

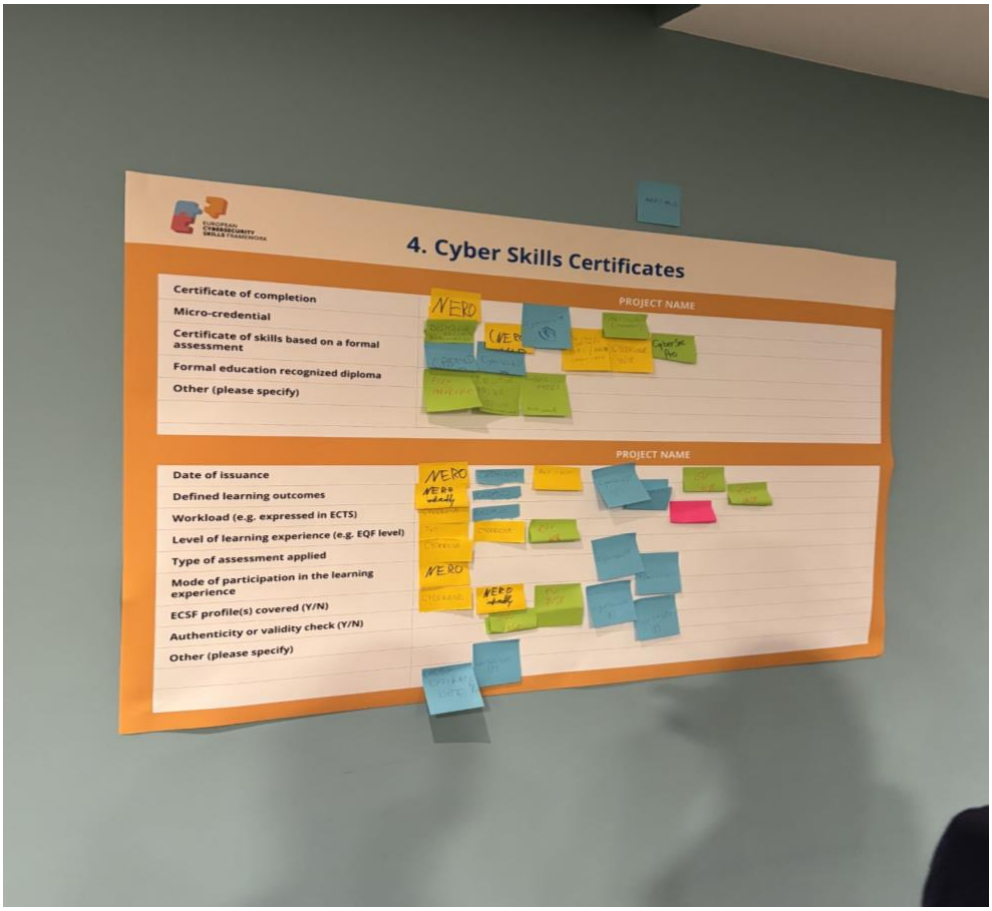


Figure 18: Photograph of the board used to collect the inputs from the participating projects on the types of Certificates

3. Ms. Kioskli and Ms. Seralidou from TRUST provided feedback on behalf of the CyberSecPro project in other themes of the interactive exercise.

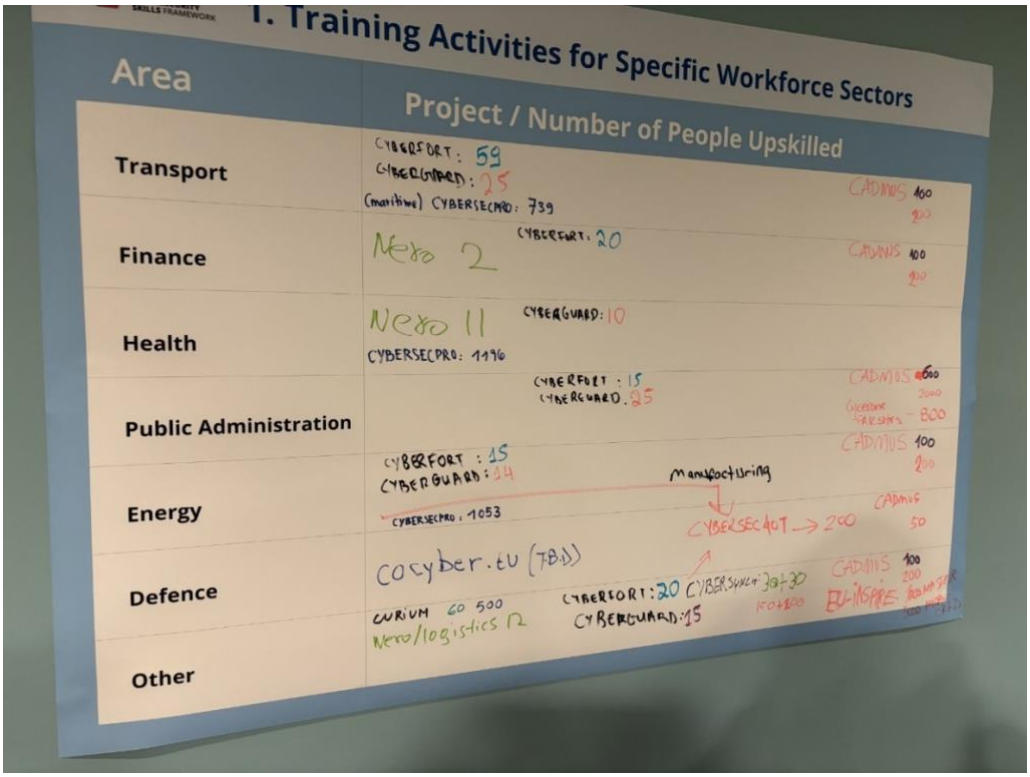


Figure 19: Photograph of the board used to collect the inputs from the participating projects on the training activities per sector

A report summarising the key insights, challenges, and recommendations emerging from the interactive exercises was created and is available to interested parties. The workshop was attended by more than 70 people, including people from ENISA, the Portuguese National Cybersecurity Centre (CNCS), the Digital Trust Centre of Excellence (DTCoE), the Agenzia per la Cybersicurezza Nazionale, Italy, the ECCC, the European Commission, and at least 17 European funded projects.

4. Mr. Ouzounis, head of the Capacity Building Unit of ENISA, participated in the Entrepreneurship and Cybersecurity event organized by CyberSecPro, on the 21st of January 2026, in Lisbon, Portugal.
5. In January 2025, the CyberSecPro project provided feedback to the public consultation of ENISA: “ENISA Guidance on technical and methodological requirements of Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 “. ENISA developed additional technical guidance for the implementation of the NIS2 cybersecurity risk management measures for the digital infrastructure sectors. The Commission Implementing Regulation (EU) 2024/2690 published 17 October 2024 lay down the rules for the application of the NIS2 Directive as regards technical and methodological requirements of the cybersecurity risk management measures and incident reporting. On this specific document, ENISA was requesting feedback in two formats: 1) though a commenting form and 2) through a set of questions. The project provided feedback through the form specifically on section 8. BASIC CYBER HYGIENE PRACTICES AND SECURITY TRAINING.

ISO, CEN/CENELEC, DIN, ETSI

Specific project partners (GUF, TRUST and APIRO) have members directly involved in standardization activities (both at national and European levels). These members attended several meetings of the working groups and committed and where possible provided information on the activities of the

CyberSecPro project. During the lifetime of the project, no opportunity was identified to directly provide feedback on the development of a standard on the specific education and training topics of the project.

Especially for ETSI, a Workshop entitled: CyberSecPro approach to training in Cybersecurity, was provided to ETSI Telecomunicación, Universidad Politécnica de Madrid, in September 2024 (2024-09-12), by the project partner GUF. The workshop included an introduction to the project, to the CyberSecPro the Syllabi and concluded with a relevant discussion with the audience.

CYS and DSA

In Cyprus, APIRO communicated and engaged with the Digital Security Authority of Cyprus (DSA) and the Cyprus Standardization Organization, in relation to the CyberSecPro project. As a result, a collaboration was established and two training courses were provided under the auspices of DSA to interested parties from the Energy and Health Sector.

National CyberSecurity Authority of Greece

The National Cybersecurity Authority of Greece, in Oct/Nov 2025, conducted an open consultation in order to update the national Cybersecurity Strategy for the years 2026-2030 . Since the national strategy addresses also the subject of cybersecurity awareness, education and training, the CyberSecPro project, reviewed the provided questions and the strategy and provided comments. The comments covered the following topics: Ideas and activities that could be added to the national Cybersecurity Strategy to increase the resilience level of Greece by 2030, the specific needs and challenges the HEI and SMEs have related to cybersecurity, which are the possible activities that the state can implement in order to effectively strengthen intelligence sharing in the field of cybersecurity, how can cybersecurity become a part of education programs in primary and secondary education and the activities (frameworks) that could be used to better align training and the needs of entities.

ECCC

The European Cybersecurity Competence Centre (ECCC), together with the Network of National Coordination Centres (NCCs), is Europe's new framework to support innovation and industrial policy in cybersecurity. This ecosystem will strengthen the capacities of the cybersecurity technology Community, shield our economy and society from cyberattacks, maintain research excellence and reinforce the competitiveness of EU industry in this field.

The Centre and the Network will make strategic investment decisions and pool resources from the EU, its Member States and, indirectly, the industry to improve and strengthen technology and industrial cybersecurity capacities, enhancing the EU's open strategic autonomy. The Centre will play a key role in delivering on the ambitious cybersecurity objectives of the Digital Europe Programme and Horizon Europe programmes.

The Centre together with the Network will support the deployment of innovative cybersecurity solutions. It will also facilitate collaboration and the sharing of expertise and capacities among all relevant stakeholders, in particular research and industrial communities, as well as public authorities, in the Community.

The CyberSecPro project has identified the key role and importance of the ECCC to cybersecurity education and training and has early on established regular interactions. The Key formal interactions are the following:

- CONVERGENCE 2023: CONVERGENCE 2023 was a two-day single-track event held over the course of 30 November – 1 December in conjunction with EU-CHECK and other partners, hosted with the friendly support of the Representation of the State of Hessen to the EU at rue Montoyer 21 in Brussels. One of the objectives in the aftermath of the four cybersecurity pilot projects is to strengthen the cybersecurity community in Europe and working to that end are representatives from TDL, the EU-CHECK (led by CNRS) and CyberSecPro projects. The evening panel of the first day of the event was dedicated to Challenges Facing the ECCC with participants: Martin Friedrich Reinhardt, Head of Unit, Affairs of the Hessian Ministry of the

Interior and for Sports, Representation of the State of Hessen to the EU, Svetla Nikova, Trust in Digital Life chair and Amardeo Sarma, Trust in Digital Life Honorary President and former chair, Tamara Tafra, Minister Counsellor for Cyber Issues, Hybrid Threats & Disinformation at PermRep of Croatia to the EU, Panagiotis Marzelas, European Security and Defence College, Claudio Teixeira, BEUC Digital Rights Legal Officer, Katarzyna Prusak–Górniak, Head of Digital Affairs Unit in Permanent Representation of Poland to the EU, Deputy Chair of the European Cybersecurity Competence Centre Governing Board and Ellen Stassart, Head of the National Cybersecurity Coordination Centre (NCC – BE).

- CONVERGENCE 2024: CONVERGENCE 2024 was a two-day single-track event held over the course of 14-15 November in conjunction with the EU-CHECK and CyberSecPro projects, hosted with the friendly support of the Representation of the State of Hessen to the EU at rue Montoyer 21 in Brussels. One of the objectives in the aftermath of the four cybersecurity pilot projects is to strengthen the cybersecurity community in Europe and working to that end are representatives from TDL, the EU-CHECK (led by CNRS) and CyberSecPro projects. The evening event included a key note address on the New European Landscape by Katarzyna Prusak–Górniak, Head of Digital Affairs Unit, Permanent Representation of the Republic of Poland to the EU; Vice Chair of the Governing Board of the European Cybersecurity Competence Centre (ECCC) and discussions (panel) with Andrea Servida, Former Head of Unit, Knowledge Management and Innovative Systems, DG CONNECT, Rodica Tirtea, Senior Policy Officer, European Cybersecurity Competence Centre (ECCC), Sébastien Ziegler, President of the IoT Forum, and European Centre for Certification and Privacy, Riccardo Masucci, Head of Brussels Office, Managing Director EU Affairs, Intel Corporation and Cornelia Kutterer, Managing Director Brussels Office, Considerati.
- Entrepreneurship and Cybersecurity event. The event, organized by CyberSecPro in January 2026, was the breeding ground for high-level discussions on cybersecurity innovation, investment perspectives, and real-world case studies, alongside experts and key stakeholders from across the ecosystem. Ms. Rodica Tirtea, Senior Policy Officer, ECCC, presented and discussed on the topic of « One European Cyber Talent Space on Standards, Skills and Education. »

Certification bodies

The main certification bodies providing international certification for cybersecurity skills are members of the Ad-Hoc Working Group on the European Cybersecurity Skills Framework (2023-2025). The CyberSecPro project was presented to all, though the discussions and presentations of the regular meetings of the group, personal interactions and in the case of ISACA, through the participation of one representative in the CONVERGANCE 2024 event presented above.

European Funded projects

Following the identification of similarly themed European funded projects, the CyberSecPro project proceeded in the design and implementation of jointly organized and clustering activities:

Workshops

- Cyber War Skills Seminar 2023, 30/11/2023, Department of Military Skills at the National Defence University, Finland with the participation of CyberSecPro partners.
- Convergence 2023, 30/11-1/12/2023, between TrustInDigitalLife (TDL), the EU-CHECK (led by CNRS) and CyberSecPro projects.
- Convergence 2024, 14-15/11/2024, between TrustInDigitalLife (TDL), the EU-CHECK (led by CNRS) and CyberSecPro projects.
- DYNAMO Cyber Morning 2023, 10/05/2023, in collaboration with the DYNAMO project.
- CyberSecPro approach to training in Cybersecurity,12/09/2024, organized by ETSI Telecomunicación, Universidad Politécnica de Madrid and CyberSecPro.
- European Cybersecurity Skills Workshop, 20-21/11/2025, powered by three DEP projects - NERO, CyberSynchrony, and CyberSecPro with support from: Infotrend Co.

- Ltd, Ianus Technologies Ltd, Maggioli S.p.A., trustilio B.V., and the University of Piraeus Research Center (UPRC).
- AI Workshop During Summer School, 15-19/07/2024, AI Workshop 2024 is a collaborative platform featuring five prominent European-funded projects: REMARKABLE, ROBUST, AIAS, DAIS, and CyberSecPro. The workshop co-located with IPICS (Intensive Programme on Information and Communication Security) 2024

Publications

Several publications to scientific journals and workshops have been jointly created and published between the CyberSecPro project and other projects. Examples of such publications are the following:

- SoK: Membership Inference is Harder Than Previously Thought, Proceedings on Privacy Enhancing Technologies 2023. The depicted work was supported by the European Union's Horizon 2020 and Horizon Europe research and innovation programmes under grant agreements No. 101083594 (CyberSecPro), No. 101070599 (SecOPERA) and No. 101007673 (RESPECT).
- Enhancing practical cybersecurity skills: The ECSF and the CyberSecPro European efforts. The research conducted in this paper was funded by the project 'A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures' (AI4HEALTHSEC) under grant agreement No 883273. The project was funded by the European Union's Horizon 2020 research and innovation programme. The authors are also grateful for the financial support provided for the 'Collaborative, Multi modal and Agile Professional Cybersecurity Training Program for a Skilled Workforce in the European Digital Single Market and Industries' (CyberSecPro) project. This project has received funding from the European Union's Digital Europe Programme (DEP) programme under grant agreement No 101083594.
- Bringing humans at the core of cybersecurity: Challenges and future research directions, Human Factors in Cybersecurity, Vol. 91, 2023, 83–92. The research conducted in this paper was funded by the project 'A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures' (AI4HEALTHSEC) under grant agreement No 883273.The project was funded by the European Union's Horizon 2020 research and innovation programme. The authors are also grateful for the financial support provided for the 'Collaborative, Multi modal and Agile Professional Cybersecurity Training Program for a Skilled Workforce in the European Digital Single Market and Industries' (CyberSecPro) project. This project has received funding from the European Union's Digital Europe Programme (DEP) programme under grant agreement No 101083594.
- Demand Analysis of the Cybersecurity Knowledge Areas and Skills for Nurses: Preliminary Findings, Proceedings of the 22nd European Conference on Cyber Warfare and Security, ECCWS 2023. The research conducted in this paper was triggered by the project 'Collaborative, Multi-modal and Agile Professional Cybersecurity Training Program for a Skilled Workforce in the European Digital Single Market and Industries' (CyberSecPro) project. This project has received funding from the European Union's Digital Europe Programme (DEP) programme under grant agreement No 101083594. The third author (KK) would also like to acknowledge the project 'A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures' (AI4HEALTHSEC) under grant agreement No 883273.
- End-to-End Encryption: Technological and Human Factor Perspectives. The research conducted in this paper was triggered by the project 'Collaborative, Multi-modal, and Agile Professional Cybersecurity Training Program for a Skilled Workforce in the European Digital Single Market and Industries' (CyberSecPro) project, which has received funding from the European Union's Digital Europe Programme (DEP) under grant agreement No. 101083594; the 'Human-centred Trustworthiness Optimization in Hybrid Decision Support' (THEMIS 5.0) project, which has received funding from the European Union's Horizon Programme under grant agreement No. 101121042; the 'Advanced Cybersecurity Awareness Ecosystem for SMEs' (NERO) project, which has received funding from the European Union's DEP

programme under grant agreement No. 101127411; the 'A Certification approach for dynamic, agile and reUSable assessmenT fOr composite systems of ICT proDucts, servicEs, and processes' (CUSTODES) which has received funding from the European Union's Horizon Programme under grant agreement No. 101120684; the 'Harmonizing People, Processes, and Technology for Robust Cybersecurity' (CyberSynchrony) project, which has received funding from the European Union's Digital Europe Programme (DEP) under grant agreement No. 101158555; and the 'Fostering Artificial Intelligence Trust for Humans towards the Optimization of Trustworthiness through Large-scale Pilots in Critical Domains' (FAITH) project, which has received funding from the European Union's Horizon Programme under grant agreement No. 101135932.

- A risk and conformity assessment framework to ensure security and resilience of healthcare systems and medical supply chain. The research conducted in this paper was triggered by the project 'Collaborative, Multi-modal, and Agile Professional Cybersecurity Training Program for a Skilled Workforce in the European Digital Single Market and Industries' (CyberSecPro) project, which has received funding from the European Union's Digital Europe Programme (DEP) under grant agreement No. 101083594; The 'Advanced Cybersecurity Awareness Ecosystem for SMEs' (NERO) project, which has received funding from the European Union's DEP programme under grant agreement No. 101127411; The 'A Certification approach for dynamic, agile and reUSable assessmenT fOr composite systems of ICT proDucts, servicEs, and processes' (CUSTODES) project, which has received funding from the European Union's Horizon Programme under grant agreement No. 101120684; The 'Harmonizing People, Processes, and Technology for Robust Cybersecurity' (CYberSynchrony) project, which has received funding from the European Union's Digital Europe Programme under grant agreement No. 101158555, supported by the European Cybersecurity Competence Centre (ECCC); The 'Fostering Artificial Intelligence Trust for Humans towards the Optimization of Trustworthiness through Large-scale Pilots in Critical Domains' (FAITH) project, which has received funding from the European Union's Horizon Programme under grant agreement No. 101135932.
- A Practical Human-Centric Risk Management (HRM) Methodology. The research conducted in this paper was triggered by the project 'Collaborative, Multi-modal, and Agile Professional Cybersecurity Training Program for a Skilled Workforce in the European Digital Single Market and Industries' (CyberSecPro) project, which has received funding from the European Union's Digital Europe Programme (DEP) under grant agreement No. 101083594; the 'Human-centred Trustworthiness Optimization in Hybrid Decision Support' (THEMIS 5.0) project, which has received funding from the European Union's Horizon Programme under grant agreement No. 101121042; the 'Advanced Cybersecurity Awareness Ecosystem for SMEs' (NERO) project, which has received funding from the European Union's DEP programme under grant agreement No. 101127411; the 'A Certification approach for dynamic, agile and reusable assessment for composite systems of ICT products, services, and processes' (CUSTODES) which has received funding from the European Union's Horizon Programme under grant agreement No. 101120684; the 'Harmonizing People, Processes, and Technology for Robust Cybersecurity' (CyberSynchrony) project, which has received funding from the European Union's Digital Europe Programme (DEP) under grant agreement No. 101158555; and the 'Fostering Artificial Intelligence Trust for Humans towards the Optimization of Trustworthiness through Large-scale Pilots in Critical Domains' (FAITH) project, which has received funding from the European Union's Horizon Programme under grant agreement No. 101135932.

It should be noted that the full list of publications of the CyberSecPro project is included in Section 3.6.

Other clustering activities

- The CyberSecPro project has published and provided (in collaboration with the CURIUM European funded project) to relevant interested parties, the Whitepaper «Comparative Analysis of Cybersecurity Incident Responder Role Across Frameworks».
- EDUCON 2025: Several members of the CyberSecPro project, together with researchers of other projects, were part of the organising committee of the conference. Moreover, a special

session on Education and Training in Cybersecurity for Professionals was co-organized with the NERO and CyberSynchrony projects. https://2025.ieee-educon.org/program/special-sessions

- EDUCON 2024: The Madeira Digital Transformation Week brought together five major events, the 30th ICE IEEE/ITMC Conference, the 2nd edition of the Madeira Digital Transformation Summit, the EIT Health Transformation Talks, the CyberSecPro Summer School and the NITIM Graduate School. This convergence of academic, policy makers and industry stakeholders provides a unique opportunity to showcase your research, projects, solutions and initiatives. This activity was supported by the following projects: AIDEAS, FAITH, XpanDH, RE4DY, AGILEHAND, AI-DAPT, TeleRehaB, Share, TEXTOUR, FITTER-EU, COMMUICTAS, SMARTBEAR, CyberSecPro, DTIM, IMPACTO and Yourimage.
- IPICS 2024– Intensive Programme on Information and Communication Security. IPICS – Intensive Programme on Information and Communication Security is a comprehensive educational initiative designed to equip participants with specialized skills and knowledge in the field of cybersecurity. These programs are structured as intensive, immersive experiences aimed at rapidly building expertise in cybersecurity concepts and practices. IPICS programs cater to individuals seeking to enter the cybersecurity industry or professionals looking to enhance their existing skills. Organized through the cooperation of CyberSecPro and CybAlliance projects.
- The 2023 Cybersecurity Hands-On-Training (CyberHOT) Summer School took place on Friday 29th of September 2023 under the auspices of NATO Maritime Interdiction Operational Training Centre (NMIOTC) after the 7th NMIOTC Cyber Security Conference in the Maritime Domain (27-28/9/23). The Summer School is co-organized by several organizations including the CyberSecPro, SENTINEL, CYRENE, IntellIOT, PHOENIIX, EnerMan SecOPERA, JCOP, REWIRE and EDGELESS projects.
- The 2024 Cybersecurity Hands-On-Training (CyberHOT) Summer School took place on Monday 9th and Tuesday 10th of September 2024 under the auspices of University of Piraeus, Research Centre (UPRC). The Summer School is co-organized by several organizations including the CyberSecPro, SecOPERA, EDGELESS, PHOENIIX, Synapse, REWIRE, CUSTODES, NERO, fAith, CYBERSYNCHRONY, Themis 5.0, RESCALE, 6gZCEL and CyberSecDome projects.
- The 5th Cybersecurity Hands-On-Training (CyberHOT) Summer School took place on Thursday 29th and Friday 30th of May 2025 under the auspices of Technical University of Crete (TUC) in Chania, Crete, Greece. The Summer School is co-organized by several organizations including the CyberSecPro, SecOPERA, EDGELESS, PHOENIIX, CYBERSYNCHRONY, Synapse, elastic, CUSTODES, fAith, Themis 5.0, RESCALE, 6gZCEL, PANDORA, INTACT, DARPA, CONSOLE, cPAID, CoEvolution, RIGOUROUS, Green.Dat.AI and CyberSecDome projects.

4.1.7 Lessons learned & Improvement

The interaction with various stakeholders has allowed the project partners to collect structured and unstructured feedback in relation to the training programme and the proposed certification schemas of the CyberSecPro project. This feedback has been utilized in shaping the evaluation (WP5) deliverables of the project. The most prominent feedback was the one extracted from the European Cybersecurity Skills Workshop, in relation to the certification of cybersecurity skills. This feedback has been included in the deliverable D5.2 and has help shape improvements to deliverable D5.3.

Conclusions

From the information presented above, it was possible to conclude that the project has reached out and engaged policy makers at national, European and International levels. Such stakeholders include ENISA, ECCC, ESCO, ECSO, the European Commission, Standards Development Organizations. These stakeholders have been presented with the key outcomes of the CyberSecPro project in relation

to training and certification. The key outcomes, recommendations and best practices of the project have been communicated through different communication channels, orally and in written format in every opportune moment. Through all of the above, the project can claim that more than 22 policy members have been engaged and that the messages of the CyberSecPro have been effectively communicated.

In relation to similarly themed European-funded projects, CyberSecPro is proud to have worked with at least 45 projects in a variety of clustering activities, such as the creation of a common whitepaper, the co-organising of workshops and conferences and the co-development and authorship of scientific work published in scientific journals and workshops.

5 Future Communication and Dissemination Activities

Communication and Dissemination Activities that are planned for the foreseeable future (beyond M38, the reporting period of this deliverable) are presented below:

Partner	Description	Dates	Location
Paper presentation at IEEE Educon 2026	SINTEF will present the paper «Virtual Realities, Real Risks: A Scoping Review for Immersive Learning in Secure Software Engineering» at 2026 IEEE Global Engineering Education Conference (EDUCON).	27-30 April 2026	Cairo, Egypt
Paper presentation at ICICT 2026	FP will present the paper "Synthetic Knowledge in Intelligent Systems: Lifecycle Models, Information Quality Degradation, and Trust-Aware Design" at the 2026 International Congress on Information and Communication Technology (ICICT2026).	24-27 February 2026	London, UK
Paper presentation at AHFE2026	FP will present the paper "Calibrating Trust in AI-Driven Cyber Defences: Human Reliance, Resistance, and Decision Dynamics" at 2026 International Conference on Applied Human Factors and Ergonomics (AHFE2026).	20-24 July 2026	Istanbul, Turkey
Paper presentation at IEEE EDUCON 2026	LAU will present a paper titled, CyberSecPro: A Modular, Industry-Aligned Approach to Cybersecurity Education in Critical Sectors	27-30 April 2026	Cairo, Egypt
Journal Publication	Partners are preparing a journal manuscript on CyberSecPro best practices, guidelines and policies		

6 KPI Overview

The following table summarises the KPIs from the Grant Agreement related to dissemination and communication with the respective partner responsible and achievements until M38 presented. Notes are shown where appropriate.

Table 7: KPI overview

KPI	Achievement (M38)	Notes
Website		
>20 website visitors monthly *{20 X 39 = 780}*	2567 (Avg: 68 monthly)	Overdelivered
>1000 site access times annually *{1000 X 3,25 = 3250}*	7897 (Avg: 2494 annually)	Overdelivered
>1000 downloads of high-quality electronic brochures with the technical approach and activities	489 for the brochure, 8206 total downloads	Overdelivered
Social Media		
5 new followers in Twitter/LinkedIn monthly {5 X 39=195}	560 (LinkedIn) 129 (X)	Overdelivered
>20 re-tweets monthly {20 X 39 = 780}	370	Underdelivered
30 LinkedIn profile views monthly {30 X 39 = 1170}	1852	Overdelivered
>30 post views monthly {30 X 39 = 1170}	7963	Overdelivered
>20 new discussions in LinkedIn	147	Overdelivered
>150 views of 5-min videos in YouTube by the end of the project	463	Overdelivered
> 10 push announcements	93 (Avg: 7 monthly)	Overdelivered
Own hosted (network) events		
5 network events (up to 25 participants)	0	A focus was placed on larger-scale events. The total number of attendees reached the number of attendees that would have been reached by including smaller events.
3 network events (25-100 participants)	4	
2 Events organised with >100 attendees	2	
Participation in events		

>20 conference/ scientific events/ industrial for presentations	Participated to 50 events so far	Overdelivered
Participation in >10 small and large-scale events	170	Overdelivered
Publications		
>15 publications in international referred publications	31 (conferences)	Overdelivered
>6 publications in international magazines	3	Underdelivered
50 Applied research papers published	56	Slightly overdelivered
Stakeholder engagement		
>10 similarly themed projects and initiatives identified	More than 140 projects and other stakeholders	
> 5 jointly organized workshops	8	Slightly overdelivered
Engagement of >7 policy making bodies	12	Slightly overdelivered
≥10 partnerships formed with key businesses in the field by the end of the project	14	As evidenced by 14 signed MoUs between public CSP partners and private institutions
Others		
Setup of CyberSecPro observatory to monitor the effectiveness of the communication strategy implemented	CSP Monitoring Tool and Admin Platform set up	Achieved
Communications starter pack on M2	Design Materials (Poster, Reports, Rollup-Banner, Social Media Account, Images, Videos, Wallpapers, Logo, Flyers	Achieved
>50 hard copies distributed in >5 events	Distributed at 6+ events (around 400-500 flyers distributed)	Overdelivered
e-Newsletter sent bi-monthly / > 8 e-newsletters	1	Discontinued after feedback at Mid-term Review (from PO)
>15 emails with rich information on project progress and DE events & opportunities	16 (sent monthly)	Achieved
>200 of the total of the participants to all events attracted and registered as contacts	Focus was placed on making participants follow CyberSecPro on Social Media rather than Newsletter (>500 followers on LinkedIn)	Achieved

6 reports produced with KPIs that are continuously monitored	16	Overdelivered

7 Conclusion

This deliverable has provided an overview of the dissemination and communication activities carried out within the CyberSecPro project. Throughout its implementation, dissemination was approached not as a formal obligation, but as a strategic instrument to enhance visibility, stakeholder engagement and long-term impact.

CyberSecPro established a coherent and recognisable project identity, supported by structured communication tools, reusable templates and a dedicated admin platform for systematic monitoring. The digital dissemination strategy proved effective in ensuring access to project results, while social media evolved into a central channel for professional outreach and engagement across academia, industry and policy communities.

Event-based dissemination and scientific publications further strengthened the project's presence within the European cybersecurity ecosystem. High-level workshops, clustering initiatives and the final conference positioned CyberSecPro as an active contributor to discussions on cybersecurity skills, training and certification.

Stakeholder engagement activities reinforced the project's policy relevance and alignment with European frameworks and initiatives. Structured interactions with standardisation bodies, certification stakeholders, national authorities and European-funded projects contributed to the credibility, interoperability and potential long-term uptake of CyberSecPro results.

An important lesson learned was the value of continuously evaluating dissemination channels and reallocating efforts towards the most effective formats. Overall, dissemination and communication within CyberSecPro have successfully supported the project's objectives and established a strong foundation for sustainability beyond its lifetime.

Annex A: Dissemination and Communication Activities

Date	Title	Location	Type	Attendees
21/11/2025	Engaging EU Projects Using the European Cybersecurity Skills Framework (ECSF) Workshop	Brussels, Belgium	Workshop	70
09/11/2025	The 17th Conference on Informatics in Education (CIE2025)	UPRC	Attendance	200
12/09/2025	ACEEU Global Forum	Prague, Czech Republic	Others	150
30/06/2025	Implementing the European Cybersecurity Skills Framework (ECSF): A Case Study of EU Innovation Projects		Paper presentation (online)	-
30/06/2025	Proposal of Harmonising Cybersecurity Professional Education and Training (CPET) in the European Union (EU): Exploratory Study		Paper presentation (on-site)	500
20/06/2025	University of Piraeus, Greece, Balkancom 2025	University of Piraeus, Greece	Paper presentation (on-site)	-
07/06/2025	Cybersecurity Certification for Professional Training: An Overview		Paper presentation (on-site)	-
09/05/2025	Implementing the European Cybersecurity Skills Framework (ECSF) for Maritime Cybersecurity Certified Professionals Using a Human-Centric Approach	Antwerp	Paper presentation (on-site)	300
08/05/2025	Cybersecurity Professional Education in the Maritime Sector	Rome	Paper presentation (on-site)	300
25/04/2025	IEEE EDUCON 2025	London, UK	Paper presentation (on-site)	-
11/04/2025	University of Pireaus dissemination - career days	Nikaia, Piraeus Greece	Others	500

Date	Title	Location	Type	Attendees
13/02/2025	Piraeus, Greece, Association of Maritime Managers in Information Technology and Communications (AM.M.I.TE.C.)	Piraeus, Greece, Association of Maritime Managers in Information Technology and Communications (AM.M.I.TE.C.)	Attendance	-
15/12/2024	Athens, Uniwa, 21sth Panhellenic Physics Conference	Athens Uniwa	Discussion panel	-
20/11/2024	Development of Cybersecurity Skills	Nicosia, Cyprus	Discussion panel	70
19/11/2024	4th Cybersecurity Stakeholder's Meeting	Nicosia, Cyprus	Discussion panel	200
15/11/2024	Convergence 2024	Representation of the State of Hessen to the EU, Brussels, Belgium	Discussion panel	50
13/11/2024	DEDEP.eu Webinar: Boost the impact of Digital Europe projects		Others	123
10/11/2024	University of Pireaus, Greece, 16th international conference on Informatics in education (CIE 2024)		Discussion panel	-
10/11/2024	University of Pireaus, Greece, 16th international conference on Informatics in education (CIE 2024)	University of Pireaus, Greece,	Paper presentation (on-site)	-
04/10/2024	Boosting SMEs Cybersecurity Resilience	Nicosia, Cyprus	Others	40
27/09/2024	3rd European Cybersecurity Skills Conference	Budapest, Hungary	Attendance	150
25/09/2024	AHWG MEETING - AHWG on European Cybersecurity Skills Framework	LUDOVIKA UNIVERSITY OF PUBLIC SERVICE, Budapest	Others	18
12/09/2024	Workshop: CyberSecPro approach to training in Cybersecurity (https://www.cybersecpro-project.eu)	ETSI Telecomunicación, Universiade Politecnica de Madrid.	Workshop	10

Date	Title	Location	Type	Attendees
13/09/2024	University of Piraeus, SETN Hellenic Conference on Informatics	University of Piraeus, SETN Hellenic Conference on Informatics	Paper presentation (on-site)	-
10/09/2024	CYBERHOT Summer School	Piraeus, Greece	Others	60
21/08/2024	Symposium on Artificial Intelligence and its Impact on Future Communities	Laurea University of Applied Sciences, Finland	Workshop	33
24/06/2024	30th ICE IEEE/ITMC Conference (conf paper 1 UPRC)	Lugo, Polemi, Rathod, Ofem	Paper presentation (on-site)	-
24/06/2024	30th ICE IEEE/ITMC Conference (Trustilio)	Rathod, Polemi	Paper presentation (on-site)	-
24/06/2024	ICE IEEE/ITMC 2024	Technology	Paper presentation (on-site)	-
20/06/2024	2nd Human Resources (HR) Living Lab		Workshop	55
12/06/2024	Maritime Conference on Cybersecurity	Athens, Greece	Attendance	-
14/06/2024	University of Piraeus, Greece, CIVEMSA 2025	University of Piraeus, Greece	Paper presentation (on-site)	-
05/06/2024	CEN/CLC/JTC 21 Working Group 2 Meetings	Online	Others	-
03/06/2024	CEN/CLC/JTC 21 Working Group 5 Meetings	Online	Others	-
24/05/2024	ETSI cybersecurity group meetings		Attendance	-
24/05/2024	CybAlliance GA Meeting and side meetings	Oslo, Norway	Discussion panel	15
21/05/2024	ENISA/ECCF SWOT Workshop		Workshop	-
16/05/2024	CEN/CLC/JTC 21 Working Group 2 Meetings	Online	Others	-
17/05/2024	47th meeting of ISO/IEC JTC 1 Information technology	Darwin, Australia and virtual	Attendance	100
13/05/2024	CEN/CLC/JTC 21 Working Group 5 Meetings	Online	Others	-

Date	Title	Location	Type	Attendees
10/05/2024	2024.ieee-educon	Kos	Workshop	30
10/05/2024	IEEE EDUCON 2024 (UPRC)		Paper presentation (on-site)	-
10/05/2024	IEEE EDUCON 2024 (UPRC, KOS)	Kos, Greece	Workshop	-
10/05/2024	IEEE EDUCON 2024 (UPRC-Paper)	Kos, Greece	Paper presentation (on-site)	-
10/05/2024	ETSI cybersecurity group meetings		Attendance	-
08/05/2024	IEEE Educon 2024 - CyberSecPro		Paper presentation (on-site)	-
08/05/2024	IEEE EDUCON 2024 (FP)	Kos, Greece	Paper presentation (on-site)	-
07/05/2024	CEN/CLC/JTC 21 Working Group 5 Meetings	Online	Others	-
10/04/2024	ENISA AHWG Meetings on Skills	Online	Others	-
08/04/2024	Presentation "Identification of threats against maritime operations" at the Maritime Forum seminar	Trondheim, Norway	Others	50
18/04/2024	ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection and its subgroups Meetings 2024 April	Manchester, UK and Berlin, Germany	Attendance	120
22/03/2024	Human Aspects of Cybersecurity Psychological factors and Performance	Riga, Latvia	Workshop	30
21/03/2024	CyberPain	Kotka Finland	Others	700
21/03/2024	CEN/CLC/JTC 13 Cybersecurity and Data Protection and subgroups Meetings 2024 March		Attendance	60
15/03/2024	NA 043 BR DIN-Normenausschuss Informationstechnik und Anwendungen (NIA) - Gemeinschafts-Lenkungsausschuss und Förderkreis	Munich, Germany	Attendance	20
12/03/2024	Digital Ship Oslo 2024	Oslo, Norway	Others	120
10/03/2024	Lamia, Greece, 20th Panhellenic Physics Conference	Lamia, Greece,	Discussion panel	-

Date	Title	Location	Type	Attendees
07/03/2024	European Cyber Security Organisation (ECSO) Board of Directors and WG 1	Brussels, Belgium	Attendance	25
06/03/2024	Human Factors and Maritime Cybersecurity: Challenges and Opportunities	Estonian Maritime Academy	Workshop	29
09/03/2024	Larisa Greece, 6ht Panhellenic Conference on Digital Culture Heritage		Paper presentation (on-site)	-
05/03/2024	ENISA Cybersecurity Standardisation Conference 2024	Brussels, Belgium	Attendance	250
28/02/2024	Opening Keynote at OCCE 2024 IFIP TC3 Open Conference on Computers in Education	Bournemouth, UK	Paper presentation (on-site)	100
26/02/2024	ECCWG		Paper presentation (on-site)	-
26/02/2024	1st Cyber Security Working Group Meeting	Lisbon, Portugal	Attendance	-
20/02/2024	ENISA AHWG Meetings on Skills	Online	Others	-
15/02/2024	DIN SK FOCUS.digital - 1st meeting	Berlin, Germany	Attendance	40
13/02/2024	CEN/CLC/JTC 21 Working Group 5 Meetings	Online	Others	-
12/02/2024	CEN/CLC/JTC 21 Working Group 2 Meetings	Online	Others	-
09/02/2024	ETSI cybersecurity group meetings		Attendance	-
09/02/2024	CYBERSECURITY EDUCATOR - IMPLEMENTING BEHAVIOURAL SCIENCE PERSPECTIVES FOR IMPROVED CYBERSECURITY AWARENESS EDUCATION IN ORGANISATIONS	European Institute for Political Studies, Chisinau, Moldova	Workshop	30
26/01/2024	ETSI cybersecurity group meetings		Attendance	-
25/01/2024	CEN/CLC/JTC 21 Working Group 1 Meetings	Online	Others	-
19/01/2024	ISACA New year event	Vilvoorde, Belgium	Attendance	150
19/01/2024	Belgium EU Presidency Cybersecurity Summit Strategic agenda for investment 2024-2030: recalibrate to new realities or implement first?	Brussels, Belgium	Discussion panel	150

Date	Title	Location	Type	Attendees
18/01/2024	CyberSecPro Event Cybersecurity education and training: (how) can we help the European Cybersecurity Competence Centre?	Representation of the State of Hessen to the EU rue Montoyer 21, 1000 Brussels, Belgium	Discussion panel	120
15/01/2024	LeADS TG3		Attendance	-
12/01/2024	ETSI cybersecurity group meetings		Attendance	-
09/01/2024	LeADS TG4		Attendance	-
08/01/2024	CEN/CLC/JTC 21 Working Group 1 Meetings	Online	Others	-
14/12/2023	European Cyber Security Organisation (ECSO) Board of Directors 2023 December	Brussels, Belgium	Attendance	30
13/12/2023	ENISA AHWG Meetings on Skills	Online	Others	-
08/12/2023	ETSI cybersecurity group meetings		Attendance	-
04/12/2023	European Cybersecurity Skills Academy, ECCO & ECSO		Workshop	-
01/12/2023	CONVERGENCE 2023	Representation of the State of Hessen to the European Union, Rue Montoyer 21 - 1000 Brussels	Discussion panel	120
30/11/2023	Cyber War Skills Seminar 2023	Finland	Paper presentation (on-site)	-
30/11/2023	The 35th Norwegian ICT Conference for Research and Education, NIKT 2023	Stavanger, Norway	Paper presentation (on-site)	-
16/11/2023	LeADS TG3		Attendance	-
14/11/2023	LeADS TG4		Attendance	-
16/11/2023	ISO/IEC JTC 1 Information technology Meeting 2023 November	Berlin, Germany	Attendance	100
10/11/2023	SEEDA-CECNSM 2023 (2)	Computer Engineering, Computer Networks	Paper presentation (on-site)	-

Date	Title	Location	Type	Attendees
10/11/2023	SEEDA-CECNSM 2023 (1)	Computer Engineering, Computer Networks	Paper presentation (on-site)	-
08/11/2023	CEN/CLC/JTC 13 Cybersecurity and Data Protection and subgroups Meetings 2023 November	ENISA, Athens, Greece	Attendance	60
02/11/2023	LeADS TG2	Trustilio	Attendance	-
27/10/2023	AI4HealthSec Meeting	Naples, Italy	Attendance	-
27/10/2023	The 17th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement	New Orleans, USA	Paper presentation (on-site)	-
25/10/2023	ISACA ATHENS CONFERENCE 2023		Paper presentation (on-site)	-
18/10/2023	DEP projects meeting event		Paper presentation (on-site)	-
19/10/2023	ETSI security conference	Sophia-Antipolis, France	Others	-
25/10/2023	ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection and its subgroups	Seoul, RoK (WG 5), online (SC 27)	Attendance	120
29/09/2023	CyberHOT Summer School, Chania, Crete, Greece	Chania, Crete, Greece Cyber	Attendance	-
29/09/2023	CyberHOT Summer School, Chania, Crete, Greece	Chania, Crete, Greece Cyber	Workshop	-
29/09/2023	10th Meeting NA 043-04-13 GA DIN/DKE Gemeinschaftsgremium Cybersecurity	Berlin, Germany	Attendance	25
28/09/2023	INFORMATIK 2023 Panel Digitale Souveränität fÜr Europa	Berlin, Germany	Discussion panel	150
27/09/2023	67th Meeting NA 043 BR DIN-Normenausschuss Informationstechnik und Anwendungen (NIA) - Gemeinschafts-Lenkungsausschuss	Cologne, Germany + online	Attendance	20
27/09/2023	NMIOTC - NATO	Chania, Greece	Discussion panel	-

Date	Title	Location	Type	Attendees
26/09/2023	LeADS TG1		Attendance	-
25/09/2023	Theia Event Roundtable "Cybersecurity in autonomous vehicles"	Porto, Portugal	Discussion panel	200
21/09/2023	European Cybersecurity Skills Conference 2023		Paper presentation (on-site)	-
21/09/2023	ENISA 2nd European Cybersecurity Skills Conference	Segovia, Spain	Paper presentation (on-site)	-
22/09/2023	10th ACM Celebration of Women in Computing (womENcourage)	Trondheim, Norway	Workshop	30
15/09/2023	LeADS TG3		Attendance	-
11/09/2023	21th ESDC EAB.Cyber Meeting	Brussels, Belgium	Attendance	-
06/09/2023	5th Cybersecurity Forum within the 32nd Economic Forum in Karpacz, Poland	Karpacz, Poland	Discussion panel	100
05/09/2023	LeADS TG4		Attendance	-
07/08/2023	The Healthcare Summit 2023		Paper presentation (online)	-
20/07/2023	Plattform Industrie 4.0: AG "Sicherheit vernetzter Systeme"	Berlin, Germany	Attendance	15
24/07/2023	The 14th International Conference on Applied Human factors and Ergonomics (AHFE2023)/Track: Human Factors in Cybersecurity	San Francisco, USA	Paper presentation (online)	6
18/07/2023	CyberSecPro Event Cybersecurity education and training: not why, but how?	Representation of the State of Hessen to the EU rue Montoyer 21, 1000 Brussels, Belgium	Discussion panel	120
21/07/2023	the 16th World Conference on Transport Research (WCTR2023)/Topic: Transport and Health	Montreal, Canada	Paper presentation (on-site)	-
11/07/2023	LeADS TG3		Attendance	-
06/07/2023	CEN/CLC/JTC 13 Cybersecurity and Data Protection		Attendance	30

Date	Title	Location	Type	Attendees
06/07/2023	LeADS TG2	Trustilio	Attendance	-
23/06/2023	22nd European Conference on Cyber Warfare and Security	Hellenic Air Force Academy Dekelia Air Force Base, Greece	Paper presentation (on-site)	120
22/06/2023	22nd ECCWS 2023- 1		Paper presentation (on-site)	-
21/06/2023	LeADS TG5		Attendance	-
16/06/2023	Cyber resilience - from research to increased European innovation		Others	-
16/06/2023	38th International Conference on Information Security and Privacy Protection		Attendance	100
13/06/2023	IFIP Technical Committee 11: Security and Privacy Protection in Information Processing Systems	Poznan, Poland	Attendance	20
08/06/2023	CyberSecPro Dissemination activities at the Finnish Emergency Services Academy's research and development days	Pelastusopisto / Emergency Services Academy Finland, Hulkontie 83, 70820 Kuopio	Workshop	-
07/06/2023	Event for the ENISA AI Conference	Brussels, Belgium	Paper presentation (on-site)	-
01/06/2023	EC-HADEA-LEADS-SPECIALISED PROJECTS Coordination Board		Workshop	15
01/06/2023	LeADS TG2	Trustilio	Attendance	-
30/05/2023	LeADS TG1		Attendance	-
28/05/2023	28th eHealth 2023 Conference		Paper presentation (on-site)	-
25/05/2023	Event for the presentation of the actions of the "Teaching and Learning Support Centre" of the University of Piraeus		Others	-

Date	Title	Location	Type	Attendees
10/05/2023	CyberSecPro collaborated with horizon innovation project DYNAMO Cyber Morning in Finland	Laurea LeppÄvaara (Vanha maantie 9, LeppÄvaara, Espoo / room Tuomo) and Cyber Morning will also be available over ZOOM.	Workshop	50
12/05/2023	ISO/IEC JTC 1 Information technology	Paestum, Italy and hybrid	Attendance	80
04/05/2023	IEEE EDUCON 2023 (Paper1 UPRC)	Ladias, Douligeris	Paper presentation (on-site)	-
04/05/2023	IEEE EDUCON 2023 (Paper2 UPRC)		Paper presentation (on-site)	-
04/05/2023	IEEE EDUCON 2023 (UPRC)	Kuwait	Paper presentation (on-site)	-
04/05/2023	LeADS TG2	Trustilio	Attendance	-
25/04/2023	LeADS TG1		Attendance	-
23/04/2023	REWIRE Project Greek INFO DAY III		Paper presentation (on-site)	-
25/04/2023	ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection and its subgroups	Redmond, Washington, USA	Attendance	120
29/10/2023	Hellenic Naval Academy: Erasmus on military digital skills	Athens, Greece	Paper presentation (on-site)	-
22/03/2023	NA 043 BR DIN-Normenausschuss Informationstechnik und Anwendungen (NIA) - Gemeinschafts-Lenkungsausschuss und Förderkreis	Berlin, Germany	Attendance	15
20/03/2023	NA 043-04 FBR "Fachbeirat Informationssicherheit"	Berlin, Germany	Attendance	20
17/03/2023	CEN/CLC/JTC 13 Cybersecurity and Data Protection and subgroups	Limassol, Cyprus	Attendance	50
14/03/2023	European Cyber Security Organisation (ECSO) Board of Directors	Brussels, Belgium	Attendance	25

Date	Title	Location	Type	Attendees
13/03/2023	CyberSecPro project presentation for the Laurea students and staff	Laurea LeppÄvaara (Vanha maantie 9, LeppÄvaara, Espoo / room Tuomo)	Discussion panel	-
02/03/2023	20th International Conference on Remote Engineering and Virtual Instrumentation (REV2023)	Thessaloniki, Greece	Others	-
01/03/2023	30 years of Department of Informatics Univ. of Piraeus	Piraeus, Greece	Others	-
28/02/2023	Meetings of NA 043-04-13 GA DIN/DKE Gemeinschaftsgremium Cybersecurity	Berlin, Germany	Attendance	25
23/02/2023	HADEA - clustering projects on advanced digital skills		Others	-
24/02/2023	DATA INDUSTRY PRACTICUM ISO Standards at American University Paris	Paris, France	Workshop	20
17/02/2023	Europe: The new era for skills - Greece: The human dynamic in the new workplace and society	Athens, Greece	Others	-
15/02/2023	"Breaking the glass ceiling" How inclusion can make the difference	ONLINE (Athens, Greece)	Others	-
15/02/2023	Meetings of NA 043-04-27 AA "Informationssicherheit, Cybersicherheit und Datenschutz" and subgroups	Berlin, Germany	Attendance	60
07/02/2023	EU Coast Guard Cybersecurity Working Group -EMSA-	EMSA - Lisbon	Workshop	30
18/01/2023	CyberSecPro Launch Event Overcoming Cyberignorance: Capabilities, Skills, and Education in Cybersecurity	Representation of the State of Hessen to the EU rue Montoyer 21, 1000 Brussels, Belgium	Discussion panel	120
11/01/2023	REWIRE Project Greek INFO DAY II		Paper presentation (on-site)	-
10/01/2023	10th Annual QED Conference on Cybersecurity, Brussels	Brussels, Belgium	Others	-
01/01/2023	Journal Paper by UPRC (Patsakis)	Intelligence	Paper presentation (on-site)	-
01/01/2023	Training sessions Chania September 2023	Chania	Paper presentation (on-site)	-

Date	Title	Location	Type	Attendees
01/01/2023	Journal paper by Trustilio (Kalogeraki, Polemi)	Polemi	Paper presentation (on-site)	-
01/01/2023	Journal paper by Trustilio (Polemi et al)	Praca, Kioskli, Becue	Paper presentation (on-site)	-
01/01/2023	SoK: Membership Inference is Harder Than Previousl	Open Access	Paper presentation (on-site)	-
01/01/2023	AHFE	Open Access	Paper presentation (on-site)	-
01/01/2023	AHFE (2)		Paper presentation (on-site)	-
01/01/2023	Journal paper by Trustilio (Karampotsis et al)	Kioskli, Tsirimpa, Dounias, Polydoropoulou	Paper presentation (on-site)	-

Annex B: Publications

Year	Authors	Title	Publisher	DOI
2023	Antreas Dionysiou and Elias Athanasopoulos	SoK: Membership Inference is Harder Than Previously Thought	Proceedings on Privacy Enhancing Technologies	https://doi.org/10.56553/popets-2023-0082
2023	Nineta Polemi & Kitty Kioskli	Enhancing practical cybersecurity skills: The ECSF and the CyberSecPro European efforts	AHFE	https://doi.org/10.54941/ahfe1003723
2023	Kitty Kioskli, Haralambos Mouratidis, Nineta Polemi	Bringing humans at the core of cybersecurity: Challenges and future research directions	AHFE	https://doi.org/10.54941/ahfe1003722
2023	Kioskli K, Tsirimpa A, Polydoropoulou A.	Human and psychosocial factors associated with natural hazard impacts and crisis response, management, and transportation: A narrative literature review.	WCTR2023	
2023	Rajamäki J, Rathod P, Kioskli K.	Demand Analysis of the Cybersecurity Knowledge Areas and Skills for the Nurses: Preliminary Findings	ECCWS2023	https://doi.org/10.34190/eccws.22.1.1181
2023	Paresh Rathod [MCA, MSc (ACSD), PhD], Jyri Rajamäki, [MSc (CS), DSc (CS), PhD], Kitty Kioskli [MSc, PhD]	CyberSecPro digital Europe innovation project: cybersecurity skills demand in the health sector	28th eHealth 2023 Conference-Human oriented approach in eHealth and digital services	
2023	Silje Berg, Tilde Thorvik and Per Håkon Meland	Fool Me Once, Shame on Me - A Qualitative Interview Study of Social Engineering Victims	NTNU	
2023	Jingyue Li, Per Håkon Meland, Jakob Svennevik Notland, André Storhaug and Jostein Hjortland Tysse	Evaluating the Impact of ChatGPT on Exercises of a Software Security Course	IEEE	https://doi.org/10.1109/ESEM56168.2023.10304857

Year	Authors	Title	Publisher	DOI
2023	Theodoros Karvounidis, Anastasios Ladias, Christos Douligeris	Assessment of Data Types and of the Ways They are Used in Scratch Using the SOLO Taxonomy	IEEE Global Engineering Education Conference (IEEE EDUCON 2023)	https://ieeexplore.ieee.org/document/10125213
2023	Maria Eftychia Angelaki, Theodoros Karvounidis, Christos Douligeris	Sustainability-Oriented Schools in Greece: Analyzing Pupils' Opinions and Perceptions About Sustainability and Redesign Computer Science Curricula Towards Green Informatics	IEEE Global Engineering Education Conference (IEEE EDUCON 2023)	https://ieeexplore.ieee.org/document/10125238
2023	Vangelis Malamas; Dimitris Koutras; Panayiotis Kotzanikolaou	Uninterrupted Trust: Continuous Authentication in Blockchain-Enhanced Supply Chains	SEEDA-CECNSM 2023	https://ieeexplore.ieee.org/abstract/document/10470549
2024	Foteini Markella Petropoulou	Cracking the Code: How Social Media and Human Behaviour Shape Cybersecurity Challenges	AHFE	
2024	Jyri Rajamäki,	LOCKing Patient Safety: A Dynamic Cybersecurity Checklist for Healthcare Workers	Academic Conferences International Limited, Curtis Farm, Kidmore End, Nr Reading, RG4 9AY, United Kingdo	https://doi.org/10.34190/eccws.23.1.2072
2024	E. Beltempo & J. Rajamäki	Implementation of the ECHO Cyber Skills Framework in the CyberSecPro Project: Enhancing Cybersecurity Capabilities	Information and Security	https://doi.org/10.11610/isij.5517
2024	Constantinos Patsakis	Integrating AI-driven Threat Intelligence and Forecasting in the Cyber Security Exercise Content Generation Lifecycle	International Journal of Information Security	
2024	Kalogeraki EM, Polemi N.	A taxonomy for Cybersecurity Standards.		
2024	Polemi N, Praca I, Kioskli K, Becue A.	Challenges and Efforts in Managing AI Trustworthiness Risks: A state of knowledge.	Frontiers in Big Data	
2024	Pinelopi Kyranoudi, Ricardo Gregorio Lugo, Nineta Polemi, Paresh Rathod, Paulinus Ofem	Sectoral Cybersecurity Skills Gap: The case of Maritime Cybersecurity Certification Training	International Conference on Engineering, Technology, and Innovation	

Year	Authors	Title	Publisher	DOI
2024	Pirinen, R., Rathod, P., & Polemi, N.	A Novel Model of the Resilient Learning in Critical Infrastructure Protection and Resilience	International Conference on Engineering, Technology, and Innovation	
2024	Karampotsis, Kioskli, Tsirimpa, Dounias, Polydoropoulou	Understanding evacuation behavior for efective disaster preparedness: a hybrid machine learning approach	Springer - Natural Hazards Journal	https://doi.org/10.1007/s11069-024-06759-y
2024	Kioskli et al	A Self-Organized Swarm Intelligence Solution for Healthcare ICT Security	15th International Conference on Applied Human Factors and Ergonomics (AHFE 2024) and the Affiliated Conferences	https://doi.org/10.54941/ahfe1004780
2024	Fotis et al.	Human Factors and Cybersecurity in NHS Virtual Wards	15th International Conference on Applied Human Factors and Ergonomics (AHFE 2024) and the Affiliated Conferences	https://doi.org/10.54941/ahfe1004782
2024	Alwaheidi et al	Integrating Human Factors into Data-driven Threat Management for Overall Security Enhancement	15th International Conference on Applied Human Factors and Ergonomics (AHFE 2024) and the Affiliated Conferences	https://doi.org/10.54941/ahfe1004778
2024	Koutras et al	The human factor impact on a Supply Chain Tracking Service through a Risk Assessment Methodology	15th International Conference on Applied Human Factors and Ergonomics (AHFE 2024) and the Affiliated Conferences	https://doi.org/10.54941/ahfe1004779
2024	Kioskli et al	Psychological Health, Resilience Outcomes and Disaster Preparedness: The Impact of Natural Hazards on Adults in Greece. A Cross-Sectional Analysis	Journal of Behavior	https://doi.org/10.47739/2576-0076/1024
2024	Rathod et al	Leveraging the European Cybersecurity Skills Framework(ECSF) in EU Innovation Projects: Workforce Development Through Skilling, Upskilling, and Reskilling	IEEE Global Engineering Education Conference (IEEE EDUCON 2024)	https://doi.org/10.1109/EDUCON60312.2024.10578846

Year	Authors	Title	Publisher	DOI
2024	Yigit et al	Enhancing Cybersecurity Training Efficacy: A Comprehensive Analysis of Gamified Learning, Behavioral Strategies and Digital Twins	IEEE 25th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)	https://doi.org/10.1109/WoWMoM60985.2024.00016
2024	Kioskli et al.	Optimizing AI System Security: An Ecosystem Recommendation to Socio-Technical Risk Management	AHFE Open Access Series	https://doi.org/10.54941/ahfe1005635
2024	Katja Henttonen; Paresh Rathod	Importance of Programming in Cybersecurity: Preliminary Findings from a Pilot Study Tailoring a Python Course for Targeted Educational Needs	IEEE	https://doi.org/10.1109/EDUCON60312.2024.10578580
2024	Dimitris Koutras, Giorgos Dimitrakopoulos, Vangelis Malamas, Panayiotis Kotzanikolaou, Christos Douligeris	Comparative Analysis and Implementation of HTTP3, MQTT, and CoAP for IoT Applications	28th Pan-Hellenic Conference on Progress in Computing and Informatics	https://doi.org/10.1145/3716554.37168
2024	Koutras Dimitris, Douligeris Christos, Panayiotis Kotzanikolaou	Comparative Analysis and Implementation of HTTP3, MQTT, and CoAP for IoT Applications	PCI 2024	
2024	Vangelis Malamas, Dimitris Koutras, Thomas K Dasaklis, Vassilis Vassilakopouls, Panayiotis Kotzanikolaou	Blockchain Revolution in the Metaverse: Challenges, Applications and Future Directions	2024 International Conference on Artificial Intelligence, Metaverse and Cybersecurity (ICAMAC)	
2024	Christos Theodoropoulos, Dimitris Koutras, Christos Douligeris, Panayiotis kotzanikolaou	An Edge Multi Factor Authentication System for Cyber Physical Systems Based on OTP	IEEE ISCC2024	

Year	Authors	Title	Publisher	DOI
2024	Nikolaos Lykousas, Constantinos Patsakis	Decoding developer password patterns: A comparative analysis of password extraction and selection practices	https://www.sciencedirect.com/science/article/pii/S0167404824002797	
2024	Constantinos Patsakis, Fran Casino, Nikolaos Lykousas	Assessing LLMs in malicious code deobfuscation of real-world malware campaigns	https://www.sciencedirect.com/science/article/pii/S0957417424017792	
2024	Tronnier, Frédéric.	Using Contextual Integrity to Uncover Acceptability of Information Flows in Central Bank Digital Currency Transactions	Proceedings of the 57th Hawaii International Conference on System Sciences	
2024	Lieberknecht, Ann-Kristin.	Exploring Determinants of Parental Engagement in Online Privacy Protection: A Qualitative Approach	Proceedings of the 2024 European Symposium on Usable Security	
2025	Kitty Kioskli, Eleni Seralidou, Nineta Polemi	A Practical Human-Centric Risk Management (HRM) Methodology	Electronics	https://doi.org/10.3390/electronics14030486
2025	Kioskli K, Grigoriou E, Islam S, Yiorkas A, Christofi L, Mouratidis M	A risk and conformity assessment framework to ensure security and resilience of healthcare systems and medical supply chain	International Journal of Information Security	https://doi.org/10.1007/s10207-025-01009-z
2025	Jyri Rajamäki, Paulinus Ofem, Annika Kallio, Miia Vakkuri	The Critical Role of Cybersecurity Education in Health Tourism	Academic Conferences International Limited	https://doi.org/10.34190/ictr.8.1.3455
2025	Leandros Maglaras, Kitty Kioskli	End-to-End Encryption: Technological and Human Factor Perspectives		https://doi.org/10.1007/978-3-031-93724-8_10
2025	Dimitris Koutras, Nikolaos Fokos, Vangelis Malamas and Panayiotis Kotzanikolaou	Cross-Protocol Experimental Assessment of BLE and RFID Vulnerabilities in IoT Devices	IEEE	
2025	Vangelis Malamas, Dimitris Koutras and Panagiotis Giannopoulos	From Detection to Decision: Adaptive Orchestration of Cyber Defense in IT/OT Converged IoT Networks	IEEE	

Year	Authors	Title	Publisher	DOI
2025	Vangelis Malamas, Dimitris Koutras, Panagiotis G. Giannopoulos	From Detection to Decision: Adaptive Orchestration of Cyber Defense in IT/OT Converged IoT Networks	12th International Conference on Internet of Things: Systems, Management and Security (IOTSMS2025)	
2025	Karvounidis Theodoros, Dimitrios Kallergis, Kitty Kioskli,Christos Douligeris	Cybersecurity Certification for Professional Training: an Overview	IEEE EDUCON 2025	
2025	Abdelkader Shaaban and Stefan Schauer	Bridging Theory and Practice forEnhanced Cybersecurity Awarenessin Critical Infrastructures		https://doi.org/10.59297/n12nnd95
2025	DLR with Ka Rannenberg	DIGITAL success stories – Bridging the cybersecurity skills gap with the CyberSecPro project	EC Directorate-General for Communications Networks, Content and Technology	
2025	Tronnier, Fédéric, Sascha Löbner, Marie-Hermance Lacombe, and Kai Rannenberg	Regulatory challenges in cybersecurity–a critical analysis of the EU AI act	IFIP World Conference on Information Security Education, pp. 80-93. Cham: Springer Nature Switzerland	
2026	Narges Arastouei, Kai Rannenberg, Danijela Boberic Krsticev	Cybersecurity Training Modules for Critical Sectors: Lessons Learned from CyberSecPro	IEEE EDUCON 2026	
2026	Per Håkon Meland	Virtual Realities, Real Risks: A Scoping Review for Immersive Learning in Secure Software Engineering	IEEE EDUCON 2026	
2026	Paulinus Ofem, Jyri Rajamäki, Katja Henttonen	CyberSecPro: A Modular, Industry-Aligned Approach to Cybersecurity Education in Critical Sectors	IEEE (EDUCON 2026)	
2026	Vangelis Malamas, Dimitris Koutras, Panagiotis Giannopoulos,Thomas K. Dasaklis	Synthetic Knowledge in Intelligent Systems: Lifecycle Models, Information Quality Degradation, and Trust-Aware Design	11th International Congress on Information and Communication Technology (ICICT2026)	

Year	Authors	Title	Publisher	DOI
2026	Vangelis Malamas, Dimitris Koutras	Calibrating Trust in AI-Driven Cyber Defences: Human Reliance, Resistance, and Decision Dynamics	17th International Conference on Applied Human Factors and Ergonomics (AHFE 2026)	
2026	Dimitris Koutras, Christos Moschos, Panagiotis Kotzanikolaou, Vangelis Malamas, and Christos Douligeris	Hardening Containerized Supply Chains: A Practical Offensive Approach Using Kubernetes	eelbe-26 _ Springer	
2026	Narges Arastouei, Cristina Alcaraz, Abdelkader Magdy Shaaban, Ruben Rios , Kai Rannenberg	CyberEducation 5.0: Transforming Cybersecurity Education into CyberSecPro		
2026	Lieberknecht, Ann-Kristin, Sascha Löbner, and Frédéric Tronnier.	More Than Mere Mediators: Examining Determinants of Parental Privacy Management Behaviors		